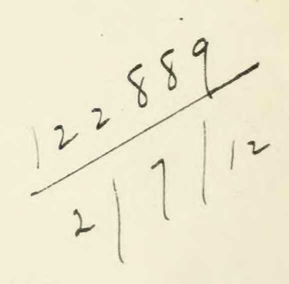


ABHANDLUNGEN ZUR GESCHICHTE DER MATHEMATISCHEN WISSENSCHAFTEN MIT EINSCHLUSS IHRER ANWENDUNGEN
BEGRÜNDET VON MORITZ CANTOR · HEFT XXVI. 2

ÜBER DAS LETZTE FERMATSCHE THEOREM

VON

BENNO LIND
IN FRANKFURT A. M.



LEIPZIG UND BERLIN
DRUCK UND VERLAG VON B. G. TEUBNER
1910

ÜBER DAS LETZTE FERMATSCHE THEOREM

VON

BENNO LIND

IN FRANKFURT A. M.

Einleitung.

Im Jahre 1670 gab der Sohn PIERRE FERMATS, SAMUEL FERMAT, eine neue Ausgabe des Diophant (L 43)[1]) mit den von seinem Vater zur BACHETchen Diophantausgabe bemerkten Randnotizen heraus. Für die in diesen Randbemerkungen enthaltenen Sätze, die wohl zu den schönsten der Zahlentheorie gehören, hatte FERMAT vorgegeben, die Beweise zu besitzen, ohne sie jedoch jemals veröffentlicht zu haben.[2]) Erst allmählich ist man dazu gelangt, die Richtigkeit dieser Sätze exakt nachzuweisen. Nur die erste der Randbemerkungen, das sogenannte letzte FERMATsche Theorem, ist bis jetzt der vollständigen Durchführung eines allgemeinen Beweises entgangen. Es ist dies der Satz, daß die Summe zweier ganzzahligen n^{ten} Potenzen $(n > 2)$ niemals gleich der n^{ten} Potenz einer ganzen Zahl sein könne. Die betreffende Randbemerkung hat bei FERMAT folgenden Wortlaut:

„Cubum autem in duos cubos, aut quadrato-quadratum in duos quadratos, et generaliter nullam in infinitam ultra quadratum, potestam in duas ejusdem nominis fas est dividere, cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.“

FERMAT hatte also behauptet, hierfür einen „wahrhaft wunderbaren“ Beweis zu besitzen. Ob dies wirklich der Fall gewesen ist, oder ob sich der geniale Mathematiker hierbei getäuscht hat, möge dahingestellt bleiben (s. L 124). Jedenfalls besitzen wir bis heute keinen exakten Beweis, trotzdem FERMAT im siebzehnten Jahrhundert gelebt hat und wir heute über ein viel größeres Untersuchungsmaterial verfügen, als es bei ihm der Fall gewesen sein kann, trotzdem die Pariser Akademie das FERMATsche Problem zweimal, 1823 und 1850, und die Brüsseler Akademie 1883 zum Gegenstand eines Preisausschreibens gewählt haben. Wie aus den Compt. Rend.

---

[1]) Diese Angaben beziehen sich auf das Literaturverzeichnis am Schluß der Abhandlung.

[2]) Der Satz, das $2^{2^k} + 1$ immer eine Primzahl sei, macht eine Ausnahme, da FERMAT hierfür keinen Beweis besaß, obgleich er an dessen Richtigkeit nicht zweifelte. Dieser Satz trifft auch nicht zu, denn, wie EULER gezeigt hat, ist schon $2^{2^5} + 1 = 4294967297 = 6700417 \cdot 641$ keine Primzahl mehr.

zu ersehen ist, erhielt die französische Akademie 1850 elf Zuschriften, von denen wohl nur die KUMMERsche verdient, einer eingehenden Betrachtung unterworfen zu werden, während fast alle anderen sogenannte „Beweise“ enthielten, die zwar keine richtigen Beweise des FERMATschen Satzes waren, wohl aber Beweise dafür, daß den Herren Verfassern mehr an der Einlösung von 3000 Frs. lag, als an der Lösung eines wissenschaftlichen Problems. Noch mehr zeigte sich dieses Moment, da durch die große Summe der Dr. WOLFSKEHLschen Stiftung die Kenntnis des Problems in die weitesten Kreise drang und hier zu tätiger Mitarbeit anregte. Aus allen Gegenden, von allen Ständen, Bauräten, Buchhaltern, Pastoren, Apothekern, Lehrern usw. trafen Lösungen ein. Alle hatten sie einen Beweis gefunden, jeder einen andern, keiner einen richtigen. Mit Recht sagt Herr NEUBERG (L 136): „La race des quadrateurs est loin d'être éteinte. En est-il de même des FERMATistes?“ — Die Zeiten der Kreisquadratur scheinen wiederkommen zu wollen. Es ist noch nicht abzusehen, welchen Aufschwung diese große kleine Literatur nehmen wird. Und dazu diese triviale Naivetät, mit der die Verfasser das Thema bearbeiten. In L 183 wird in einer Anmerkung gesagt: „Die meisten Autoren fallen mit der Tür ins Haus. Die Art, wie sie die Behandlung eines Gegenstandes beginnen, läßt den nicht unterrichteten Leser glauben, daß noch nie vorher jemand über diesen Gegenstand geschrieben habe.“ Das Gleiche bemerkt Herr NEUBERG an genannter Stelle. — Mit welchen bahnbrechenden Theorien diese Herrn Autoren kommen, zeigt L 66. Wie sich der Verfasser in einem Vorwort ausdrückt, stützt sich der dargebotene Beweis auf folgenden Grundgedanken: „Soll die Gleichung $ap + q = as$ für ganze Zahlen bestehen, so muß auch die Zahl q durch a teilbar sein. Kann man nachweisen, daß q die Zahl a als Faktor nicht enthalten kann, so hat man dadurch bewiesen, daß jene Gleichung für ganze Zahlen unmöglich bestehen kann.“ Solchen Ausführungen gegenüber ist es wirklich an der Zeit, klarzumachen, was das FERMATsche Problem, wenigstens in seiner elementaren Ausdehnung, bedeutet. Der Zweck der vorliegenden Abhandlung soll sein, alles auf diesem Gebiete in elementarer Hinsicht Geleistete, das ich in möglichst vereinfachter Form darstelle, und dem ich meine eigenen Untersuchungen[1]) beifüge, zusammenzufassen und einen Überblick zu geben, auf welchem Stand heute das FERMATsche Problem angelangt ist, und wo Wege zu einem Beweise offenstehen oder zum Teil angebahnt sind. Wie wir in dem anschließenden geschichtlichen Teil sehen werden, wäre oft viel Arbeit erspart worden, wenn die Bearbeiter des Themas Kenntnis von früheren

---

[1]) Dieselben sind, sofern sie nicht schon in einer früheren Abhandlung enthalten sind, mit * versehen.

Untersuchungen gehabt hätten. In diesem Teile berichtige ich auch verschiedene mir zur Hand gekommene „Beweise“, muß jedoch, wie auch im ausführenden Teil, auf die eingehende Betrachtung der mittels der Theorie der n^{ten} Einheitswurzeln und der komplexen Zahlen gewonnenen Methoden, insbesondere auf die klassischen Arbeiten KUMMERS, verzichten, da diese einen zu großen Raum erforderten (ich verweise hier auf L 64). Leider konnten auch in diesem Teile nicht alle im Literaturverzeichnis enthaltenen Abhandlungen aufgenommen werden, da es mir nicht möglich war, sämtliche bezügliche Schriften zu erhalten.

Frankfurt am Main, 11. April 1909.

1. Über die Gleichung $x^n + y^n = z^n$.

I. Ist die Existenz der Gleichung

$$x^n + y^n = z^n \tag{1}$$

in ganzen positiven Zahlen zu untersuchen, so kann man ohne Einschränkung der Allgemeinheit x, y und z als relativ prim annehmen; denn hätten zwei dieser Zahlen einen gemeinschaftlichen Faktor, so müßte ihn auch die dritte enthalten, und die Gleichung wäre durch die n^{te} Potenz dieses Faktors teilbar. Ferner kann man n als Primzahl annehmen, da jede Potenz von der Form a^{mn} gleich $(a^m)^n$ ist, und zwar muß n, wie wir im folgenden sehen werden, eine ungrade Primzahl sein. Aus (1) ist weiterhin ersichtlich, daß eine der Unbekannten grade und die beiden andern ungrade sein müssen. Nun besteht der Satz, dessen Herleitung hier wohl unnötig sein wird:

(2) Sind x und y teilerfremd und n eine ungrade Primzahl, so sind die beiden Faktoren von $x^n \pm y^n$, $x \pm y$ und $\frac{x^n \pm y^n}{x \pm y} = x^{n-1} \mp x^{n-2} y + \cdots + y^{n-1}$, entweder relativ prim, oder sie haben den größten gemeinschaftlichen Teiler n, der in $\frac{x^n \pm y^n}{x \pm y}$ nur in der ersten Potenz enthalten ist.

Angenommen, es sei $x^n + y^n = z^n$, so ist das Produkt der beiden Faktoren $x + y$ und $\frac{x^n + y^n}{x + y}$ gleich z^n. Es muß also, wenn keiner dieser Faktoren durch n teilbar ist, jeder von ihnen eine n^{te} Potenz sein. Im andern Falle wäre $x + y$ von der Form $n^{n-1}c^n$ und $\frac{x^n + y^n}{x + y}$ von der Form $n\gamma^n$. Dasselbe gilt für $z - x$ und $\frac{z^n - x^n}{z - x}$ und für $z - y$ und $\frac{z^n - y^n}{z - y}$, so daß wir den Satz aufstellen können:

(3) Ist die Gleichung $x^n + y^n = z^n$ in ganzen Zahlen lösbar, und gelten die oben gestellten Bedingungen, so sind die Unbekannten x, y, z durch eine der folgenden drei[1]) Relationsgruppen darstellbar, wobei $\varphi(x, y)$, $\varphi(z, x)$,

---

[1]) Wegen der Homogenität von (1) in x und y wird der Fall, daß y durch n teilbar ist, gar nicht erwähnt.

$\varphi(z, y)$ die entsprechenden Ausdrücke für $\frac{x^n + y^n}{x + y}$, $\frac{z^n - x^n}{z - x}$, $\frac{z^n - y^n}{z - y}$ bezeichnen:

$$
\text{(I)} \begin{cases}
\text{(a)} & z - y = a^n, \quad z - x = b^n, \quad x + y = c^n, \\
\text{(b)} & \varphi(z, y) = \alpha^n, \quad \varphi(z, x) = \beta^n, \quad \varphi(x, y) = \gamma^n, \\
\text{(c)} & x = a\alpha, \quad y = b\beta, \quad z = c\gamma, \\
& x = \frac{1}{2}(c^n - b^n + a^n), \\
\text{(d)} & y = \frac{1}{2}(c^n + b^n - a^n), \\
& z = \frac{1}{2}(c^n + b^n + a^n);
\end{cases}
$$

$$
\text{(II)} \begin{cases}
\text{(a)} & z - y = n^{n\lambda - 1}a^n, \quad z - x = b^n, \quad x + y = c^n, \\
\text{(b)} & \varphi(z, y) = n\alpha^n, \quad \varphi(z, x) = \beta^n, \quad \varphi(x, y) = \gamma^n, \\
\text{(c)} & x = n^\lambda a\alpha, \quad y = b\beta, \quad z = c\gamma, \\
& x = \frac{1}{2}(c^n - b^n + n^{n\lambda - 1}a^n), \\
\text{(d)} & y = \frac{1}{2}(c^n + b^n - n^{n\lambda - 1}a^n), \\
& z = \frac{1}{2}(c^n + b^n + n^{n\lambda - 1}a^n);
\end{cases}
$$

$$
\text{(III)} \begin{cases}
\text{(a)} & z - y = a^n, \quad z - x = b^n, \quad x + y = n^{n\lambda - 1}c^n, \\
\text{(b)} & \varphi(z, y) = \alpha^n, \quad \varphi(z, x) = \beta^n, \quad \varphi(x, y) = n\gamma^n, \\
\text{(c)} & x = a\alpha, \quad y = b\beta, \quad z = n^\lambda c\gamma \\
& x = \frac{1}{2}(n^{n\lambda - 1}c^n - b^n + a^n), \\
\text{(d)} & y = \frac{1}{2}(n^{n\lambda - 1}c^n + b^n - a^n), \\
& z = \frac{1}{2}(n^{n\lambda - 1}c^n + b^n + a^n).
\end{cases}
$$

Hierbei sind a, b, c, α, β, γ zu zweien untereinander und zu n relativ prim. Eine der Größen a, b, c ist grade, die beiden andern sind ungrade, während α, β, γ alle drei ungrade sind. n^λ stellt die höchste Potenz von n dar, die in x bzw. z enthalten ist, die, wie sich später zeigen wird, den Mindestwert n^2 besitzt (s. III.).

Im folgenden wird allgemein der Fall (I) betrachtet. Nur wo die beiden andern Fälle bemerkenswerte Abweichungen bieten, werden diese besonders untersucht. —

II. Nach dem kleinen Fermatschen Satze bestehen die Kongruenzen:

$$x^n \equiv x, \; y^n \equiv y, \; z^n \equiv z \pmod{n}.$$

Da nach (1)

$$x^n + y^n - z^n \equiv 0 \pmod{n}$$

ist, so ist auch:

(4) $k = x + y - z \equiv 0 \pmod{n}$. (L 6, 20, 103, 106, 107, 151, 156, 160)

Da aber

$$(5)\qquad 2k = c^n - b^n - a^n$$

ist, so muß ebenso die Kongruenz statthaben:

$$(6)\qquad c - b - a \equiv 0 \pmod{n}.$$

Nun findet man aus (Id), (4) und (5)

$$(7)\qquad \begin{cases} x \equiv a^n \equiv a \pmod{n} \\ y \equiv b^n \equiv b \quad \text{„} \\ z \equiv c^n \equiv c \quad \text{„} \end{cases} \qquad \text{(L 6, 103, 106, 107)}$$

und hieraus durch Potenzieren:

$$\begin{aligned} x^n &\equiv a^n \pmod{n^2} \\ y^n &\equiv b^n \quad \text{„} \\ z^n &\equiv c^n \quad \text{„} \quad . \end{aligned}$$

Durch Addition erhält man dann mit (1):

$$(8)\qquad \frac{c^n - b^n - a^n}{2} = k = x + y - z \equiv 0 \pmod{n^2}. \qquad \text{(L 6, 103, 106, 107)}$$

Nimmt man jetzt allgemein an, es sei

$$(9)\qquad k \equiv 0 \pmod{n^\lambda},$$

wobei λ eine ganze positive Zahl $\geqq 2$ bedeutet, so ergibt sich aus:

$$(10)\qquad \begin{cases} 2x = 2a\alpha = c^n - b^n + a^n = 2a^n + (c^n - b^n - a^n), \\ 2y = 2b\beta = c^n + b^n - a^n = 2b^n + (c^n - b^n - a^n), \\ 2z = 2c\gamma = c^n + b^n + a^n = 2c^n - (c^n - b^n - a^n), \end{cases} \qquad \text{(L 107)}$$

daß:

$$(11)\qquad \begin{cases} x \equiv a^n \pmod{n^\lambda} \\ y \equiv b^n \quad \text{„} \\ z \equiv c^n \quad \text{„} \quad . \end{cases} \qquad \text{(L 107)}$$

Jetzt verallgemeinere man die Kongruenzen (7) auf mod n^μ, dann erhält man durch Potenzieren:

$$(12)\qquad x^n \equiv a^n,\ y^n \equiv b^n,\ z^n \equiv c^n \pmod{n^{\mu+1}}.$$

(Man sieht leicht, daß die Modulpotenz $\mu + 1$ bei diesen drei Kongruenzen gleich sein muß.) Dadurch wird aber auch

$$c^n - b^n - a^n \equiv 0 \pmod{n^{\mu+1}}$$

und man erkennt, daß $\mu + 1 = \lambda$ sein muß. Es ergibt sich dann aus (11) und (12)

$$x^n \equiv x \pmod{n^\lambda}$$

und man hat allgemein die wichtigen Kongruenzen:

$$
\begin{aligned}
x^{n-1} &\equiv 1 \pmod{n^\lambda} \\
y^{n-1} &\equiv 1 \quad\text{,,} \\
z^{n-1} &\equiv 1 \quad\text{,,}\ ,
\end{aligned}
\tag{13*}
$$

wobei also λ mindestens gleich 2 ist. Ebenso erhält man aus (11) und (13):

$$
\begin{aligned}
a^{n(n-1)} &= (z-y)^{n-1} \equiv 1 \pmod{n^\lambda} \\
b^{n(n-1)} &= (z-x)^{n-1} \equiv 1 \quad\text{,,} \\
c^{n(n-1)} &= (x+y)^{n-1} \equiv 1 \quad\text{,,}\ .
\end{aligned}
\tag{14*}
$$

Nun ist nach dem Vorhergehenden identisch:

$$
\begin{aligned}
k &= x + y - z \\
&= x - a^n \\
&= y - b^n \\
&= c^n - z \quad ;
\end{aligned}
\tag{15} \qquad \text{(L 6)}
$$

nach (I c) wird also k durch a, b und c teilbar sein, und man kann setzen:

$$c^n - b^n - a^n = 2k = 2n^\lambda abcd, \tag{16}$$

folglich wird:

$$
\begin{aligned}
x &= a^n + n^\lambda abcd, \\
y &= b^n + n^\lambda abcd, \\
z &= c^n - n^\lambda abcd,
\end{aligned}
\tag{17}
$$

oder nach Teilung durch a, bzw. b und c:

$$
\begin{aligned}
\alpha - a^{n-1} &= n^\lambda bcd, \\
\beta - b^{n-1} &= n^\lambda acd, \\
\gamma - c^{n-1} &= -n^\lambda abd.
\end{aligned}
\tag{18}
$$

Nach (12) besteht dann wegen Satz (2) die Kongruenz:

$$x \equiv a \pmod{n^{\lambda-1}},$$

in der man durch a dividieren kann. So entstehen die neuen bemerkenswerten Formeln:

$$
\begin{aligned}
\alpha &\equiv 1 \pmod{n^{\lambda-1}}, \\
\beta &\equiv 1 \pmod{n^{\lambda-1}}, \\
\gamma &\equiv 1 \pmod{n^{\lambda-1}},
\end{aligned}
\tag{19*}
$$

und:

$$a^{n-1} \equiv b^{n-1} \equiv c^{n-1} \equiv 1 \pmod{n^{\lambda-1}}, \tag{20*}$$

welch letztere durch Potenzieren die Kongruenzen (14) bestätigen. —

III.* Bei den vorangegangenen Formeln war angenommen worden, es sei keine der Zahlen x, y, z durch n teilbar. Für den Fall, daß eine der-

selben durch n teilbar ist, für den wir (III) wählen, setze man an die Stelle von c^n, γ^n, $c\gamma$ resp. $n^{n\lambda-1}c^n$, $n\gamma^n$, $n^\lambda c\gamma$. Die Formeln für x und y, bzw. a und b ändern sich überhaupt nicht. Dagegen gilt bei (13) nur $z^n \equiv z \pmod{n^\lambda}$[1]), was ja selbstverständlich ist; ebenso bei den entsprechenden Kongruenzen in (14) und (20). Da nun $k = n^{n\lambda-1}c^n - n^\lambda c\gamma$ ist, so kann z durch keine höhere Potenz von n teilbar sein als k und umgekehrt. -- Kongruenzen wie

(21) $$a^n + b^n \equiv 0 \pmod{n^\lambda}$$

verstehen sich von selbst.

Nun steht es in Frage, ob (19) für γ auch hier gilt. Zum Zwecke dieser Untersuchung setze man die Werte von (IIId) in (1) ein:

$$[(a^n + b^n) + n^{n\lambda-1}c^n]^n = [n^{n\lambda-1}c^n + (b^n - a^n)]^n + [n^{n\lambda-1}c^n - (b^n - a^n)]^n$$

und entwickele dies in:

(1b) $$\begin{aligned}&(a^n + b^n)^n + (a^n + b^n)^{n-1}n^{n\lambda}c^n + n^{2n\lambda-1}P_1\\ &= 2(b^n - a^n)^{n-1}n^{n\lambda}c^n + n^{2n\lambda-1}(P_2 + P_3),\end{aligned}$$

wobei $n^{2n\lambda-1}P_1$, $n^{2n\lambda-1}P_2$, $n^{2n\lambda-1}P_3$ die Fortsetzungen der Binomialentwicklungen darstellen. Da nun:

$$a^n + b^n = 2n^\lambda c\gamma - n^{n\lambda-1}c^n,$$

so ist die linke Seite von (1b) $\equiv 2^n n^{n\lambda}c^n\gamma^n \pmod{n^{\lambda(2n-1)}}$, woraus für (1b) hervorgeht:

$$2(b^n - a^n)^{n-1}n^{n\lambda}c^n \equiv 2^n n^{n\lambda}c^n\gamma^n \pmod{n^{\lambda(2n-1)}},$$

oder

$$2(b^n - a^n)^{n-1} \equiv 2^n\gamma^n \pmod{n^{n\lambda-\lambda}}.$$

Da aber

$$b^n - a^n = y - x$$

und nach (IIIa)

$$y \equiv -x \pmod{n^{n\lambda-1}},$$

so kann man y für $-x$ setzen und erhält

$$2(2y)^{n-1} \equiv 2^n\gamma^n \pmod{n^\lambda}$$

und folglich nach (13)

$$\gamma^n \equiv 1 \pmod{n^\lambda}$$

und wegen (2)

$$\gamma \equiv 1 \pmod{n^{\lambda-1}},$$

wodurch das in (19) erhaltene Resultat auch für den Fall (III) Gültigkeit erlangt. —

(22) Ist $x + y$ durch $n^{n\pi}$, so ist es auch durch $n^{n(\pi+1)-1}$ teilbar. (L 20, 21).

---

[1]) Nicht $z^{n-1} \equiv 1 \pmod{n^\lambda}$!

Es sei

$$x + y = n^{n\pi} e$$
$$z = n^{\pi} e',$$

so wird aus (1):

$$(n^{n\pi} e - y)^n + y^n = n^{n\pi} e'^n$$

oder

$$n^{2n\pi+1} e^2 \cdot P_1 + n^{n\pi+1} e \cdot y^{n-1} = n^{n\pi} e'^n,$$
$$n^{n\pi+1} e^2 \cdot P_1 + n e y^{n-1} = e'^n.$$

Es müßte also e' den Faktor n noch einmal enthalten, und man hätte, wenn man $e' = n e''$ setzt:

$$n^{n\pi+1} e^2 P_1 + n e y^{n-1} = n^n e''^n;$$

folglich wäre

$$e \equiv 0 \pmod{n^{n-1}}$$

d. h.:

$$x + y \equiv 0 \pmod{n^{n(\pi+1)-1}}.$$

(22) kann man auch aus der Tatsache herleiten, daß $x + y$ von der Form $n^{n-1} (n^{\pi} c)^n$ sein muß.

Durch gleichen Beweis erhält man:

(23) Ist $x + y$ durch $p^{n\pi+1}$ teilbar, wobei p eine von n verschiedene Primzahl ist, so ist es auch teilbar durch $p^{n(\pi+1)}$. (s. L 20).

Dieser Satz folgt auch direkt aus (Ia)—(IIIa). —

IV. (24)* Ist $n = 2rm + 1$, und ist $p = 2r + 1$ eine Primzahl, so besteht für jede Zahl x immer die Kongruenz

(24) $$x^n \equiv x \pmod{p}.$$

Sei nämlich x nicht durch p teilbar, so ist nach dem Fermatschen Lehrsatz:

$$(x^m)^{p-1} \equiv 1 \pmod{p}$$

oder

$$x^{n-1} \equiv 1 \pmod{p}.$$

Für eine durch p teilbare Zahl ist (24) selbstverständlich.

Ist nun $r = 1$, so kann n immer eine Primzahl sein. Es besteht demnach für jede ungerade Primzahl n die Kongruenz:

(25) $$x^n \equiv x \pmod{3}.$$ (L 6)

Hieraus kann man wie bei (4) folgern, daß wegen (1) die Kongruenz statt hat:

(26) $$x + y - z \equiv 0 \pmod{3},$$ (L 6)

und auf die gleiche Art und Weise, wie in II. geschildert worden ist, kann man dann die Kongruenzen herleiten:

(27)* $$k \equiv 0 \pmod{9}$$

(28)* $$\begin{cases} x \equiv a^n \pmod 9 \\ y \equiv b^n \quad ,, \\ z \equiv c^n \quad ,, \end{cases}$$

(29)* $$\begin{cases} x^n \equiv x \quad ,, \\ y^n \equiv y \quad ,, \\ z^n \equiv z \quad ,, \end{cases}$$

(30)* $$\begin{cases} (x+y)^n \equiv x+y \pmod 9 \\ (z-x)^n \equiv z-x \quad ,, \\ (z-y)^n \equiv z-y \quad ,, \end{cases}$$

(31)* $$\alpha \equiv \beta \equiv \gamma \equiv 1 \pmod 3.$$

Auch diese Kongruenzen können, wie in II., auf mod 3^λ erweitert werden.

Die hier für $r = 1$, also für $p = 3$ entwickelten Kongruenzen gelten für alle den in (24) gestellten Bedingungen genügenden Primzahlen p und n.

V.* (32)* Die Unbekannten müssen größer als das 54fache Quadrat des Exponenten sein.

Stellt man den Ausdruck k nach (16), wobei $\lambda = 2$ angenommen wird, in die Gleichung

(33) $$x + y = z + n^2abcd,$$

so sieht man unter der Annahme $y > x$, daß x nicht kleiner als n^2abcd sein kann, da sonst die rechte Seite größer als die linke ist. Es muß also x und a fortiori y und $z > n^2abcd$ sein. Unter diesen Annahmen kann man mit Berücksichtigung von (16) und (27) folgende Skala aufstellen:

(34)* $$x + y > z > y > \frac{x+y}{2} > x > 9abcn^2 \geqq 9 \cdot 6n^2. —$$

(35)* $y - x$ muß größer als $2^n - 1$ sein.

Nach (Ia) ist

(36) $$y - x = b^n - a^n.$$

Der Mindestwert von a ist 1, der von $b > a$ ist 2. Es wäre demnach bei kleinsten a und b:

$$y - x = 2^n - 1,$$

während bei den andern Fällen die Differenz von y und x größer als die genannte sein muß. —

(37)* z liegt zwischen x und $x\frac{n}{n-1}$ oder zwischen y und $y\frac{n}{n-1}$. x und y liegen zwischen z und $\frac{n-1}{n}z$.

Besteht die Gleichung (1), so kann man durch Division eine ähnliche Gleichung in Brüchen erhalten. Angenommen, wir hätten die Gleichung[1])

$$\left(\frac{x_1}{x_2}\right)^n + \left(\frac{y_1}{y_2}\right)^n = \left(\frac{z_1}{z_2}\right)^n = \left(\frac{x_1}{x_2} + \frac{u_1}{u_2}\right)^n = \left(\frac{x_1}{x_2}\right)^n + \binom{n}{1}\left(\frac{x_1}{x_2}\right)^{n-1}\frac{u_1}{u_2} + \cdots + \left(\frac{u_1}{u_2}\right)^n,$$

und es sei darin $\frac{x_1}{x_2} > n$, so folgt bei der Annahme

$$\frac{u_1}{u_2} \geqq 1$$

aus der Gleichung

$$\left(\frac{y_1}{y_2}\right)^n = n\left(\frac{x_1}{x_2}\right)^{n-1}\frac{u_1}{u_2} + \cdots,$$

daß:

$$\left(\frac{y_1}{y_2}\right)^n > n\left(\frac{x_1}{x_2}\right)^{n-1} > n \cdot n^{n-1}$$

d. h.

$$\frac{y_1}{y_2} > n.$$

Ist $\frac{x_1}{x_2}$ aber $\gtreqless n$, so muß nach:

$$\left(\frac{y_1}{y_2}\right)^n > n\left(\frac{x_1}{x_2}\right)^{n-1} > \frac{x_1}{x_2} \cdot \left(\frac{x_1}{x_2}\right)^{n-1}$$

auch

$$\frac{y_1}{y_2} > \frac{x_1}{x_2} \quad \text{sein.}$$

Ist nun $\frac{y_1}{y_2} \gtreqless n$, so muß nach dem gleichen Verfahren $\frac{x_1}{x_2} > \frac{y_1}{y_2}$ und nach dem Vorhergehenden $\frac{y_1}{y_2} > \frac{x_1}{x_2}$ sein. Es kann daher nur eine dieser Zahlen $\gtreqless n$ sein, die andere aber $> n$. Daraus folgt wiederum, daß auch die erste $> n$ sein muß.

Dies kann aber nur gelten, wenn $\frac{u_1}{u_2} \geqq 1$ ist. Kann man nun (1) durch eine Zahl so dividieren, daß die erhaltenen Brüche $\leqq n$ sind und $\frac{z_1}{z_2} - \frac{x_1}{x_2}$ oder $\frac{z_1}{z_2} - \frac{y_1}{y_2} \geqq 1$ ist, so ist die ursprüngliche Gleichung unmöglich. Damit nun $\frac{u_1}{u_2}$ möglichst groß werde, sei der größte der Brüche $= n$, d. h., man hat die Gleichung durch $\frac{z}{n}$ zu dividieren. Damit jetzt die Gleichung möglich ist, muß z. B. $\frac{z_1}{z_2} - \frac{x_1}{x_2} < 1$ sein. Nun heißt die gefundene Gleichung:

$$\left(\frac{xn}{z}\right)^n + \left(\frac{yn}{z}\right)^n = n^n.$$

1) Der erste Teil des folgenden Verfahrens ist L 59 entnommen.

Es muß daher

$$n - \frac{xn}{z} < 1 \tag{37a}$$

oder

$$z < \frac{xn}{n-1}$$

sein, damit die Gleichung (1) möglich sei. Da $z > x$ ist, kann man die Grenzen für z ziemlich genau aus x und n bestimmen, denn man hat:

$$x\frac{n}{n-1} > z > x\frac{n}{n}. \tag{38)*}$$

Umgekehrt lassen sich ebenso enge Grenzen für x ziehen, denn aus (37a) folgt auch:

$$z\frac{n}{n} > x > z\frac{n-1}{n}. \tag{39)*}$$

Die entsprechenden Relationen lassen sich in gleicher Weise für y ableiten.

Aus (37a) gehen folgende Ungleichungen hervor:

$$\begin{aligned} z &> n(z-x) = nb^n \\ y &> nb^n - a^n \\ x &> (n-1)\,b^n. \end{aligned} \tag{40)*}$$

Setzt man hier die kleinsten Werte von a und b, nämlich 1 und 2 ein, so erhält man:

$$z > n\,2^n; \qquad y > n\,2^n - 1; \qquad x > (n-1)\,2^n. \tag{41)*}$$

So hat man z. B. bei $n = 101$ für die kleinste Zahl:

$$x > 253530120045645880299340641075200,$$

während aus (34) nur $x > 550854$ hervorgeht. Für die Fälle (II) und (III) sieht man leicht, daß sogar $x > n^{2n}$ sein muß. —

VI. Man kann immer drei Zahlen x, y, z folgendermaßen in Summen von drei anderen zerlegen:

$$z = c' + b' + a', \quad y = c' + b', \quad x = c' + a' \tag{42}$$ (L 15, 179)

wobei c', b', a' die Werte besitzen:

$$a' = a^n, \qquad b' = b^n, \qquad c' = k. \tag{43}$$

Drückt man z durch diese Werte in (1) aus, so wird:

$$(z - b')^n + (z - a')^n = z^n \tag{44}$$

oder

$$z^n - \binom{n}{1} z^{n-1}(b' + a') + \cdots - (b'^n + a'^n) = 0.$$

Ebenso kann man (1) durch y und x darstellen und erhält zwei (44) ähnliche Gleichungen, aus denen man erkennt, daß:

$$(45)\qquad \begin{aligned} b'^n + a'^n &\equiv 0 \pmod z \\ (b' - a')^n + a'^n &\equiv 0 \pmod y \\ (b' - a')^n - b'^n &\equiv 0 \pmod x. \end{aligned} \qquad \text{(L 15)}$$

—

Da x, y und z keinen gemeinschaftlichen Teiler haben, so kann man annehmen, daß:

$$(46)\qquad z = a_1 x + b_1 y, \qquad \text{(L 126)}$$

und man erhält aus $x^n + y^n = (a_1 x + b_1 y)^n$ oder:

$$(a_1^n - 1) x^n + (b_1^n - 1) y^n + \binom{n}{1} a_1^{n-1} x^{n-1} b_1 y + \cdots = 0,$$

daß:

$$(47)\qquad \begin{aligned} a_1^n &\equiv 1 \pmod y \\ b_1^n &\equiv 1 \pmod x). \end{aligned} \qquad \text{(L 126)}$$

(47) gilt auch für Brüche a_1 und b_1, wenn man z. B. in der Gleichung:

$$(48)\qquad c_1 z = a_1 x + b_1 y$$

durch c_1 dividiert. Solche Gleichungen wie (45) und (48) kann man leicht aus (I) usw. finden. Es genügt auch, wenn man durch beliebige Werte von a_1 und b_1 in der Gleichung

$$a_1 x + b_1 y = c_1$$

die Größe c_1 feststellt und dann aus

$$\left(\frac{a_1 z}{c_1}\right) x + \left(\frac{b_1 z}{c_1}\right) y = z$$

die entsprechende Relation (47) ableitet. —

Aus der Entwickelung der Gleichung

$$x^n + (c^n - x)^n = c^n \gamma^n$$

erhält man die Kongruenz:

$$(49)^*\qquad \gamma^n - n x^{n-1} \equiv 0 \pmod{c^n}$$

und ebenso

$$\gamma^n - n y^{n-1} \equiv 0 \pmod{c^n}.$$

Auf ähnliche Weise erhält man:

$$(50)^*\qquad \begin{aligned} \alpha^n - y^{n-1} &\equiv 0 \pmod z, \\ \beta^n - x^{n-1} &\equiv 0 \quad \text{,,} \quad . \end{aligned}$$

Aus (49) und (50) gehen wieder nacheinander hervor:

$$(51)^*\qquad \gamma^n - n\alpha^n \equiv \gamma^n - n\beta^n \equiv 0 \pmod c,$$

$$(52)^*\qquad \beta^n - \alpha^n \equiv 0 \quad \text{,,}$$

(53)* $$\beta^n - y^{n-1} \equiv \alpha^n - x^{n-1} \equiv 0 \pmod{c},$$

(54)* $$x \equiv -y \equiv a^n \equiv -b^n \quad " \quad .$$

Analoge Kongruenzen kann man mod a und mod b aufstellen.

Im Falle (III) ändern sich einige dieser Kongruenzen wie:

(49a)* $$\gamma^n - x^{n-1} \equiv 0 \pmod{n^{n\lambda-1} c^n},$$

(51a)* $$\gamma^n - \alpha^n \equiv 0 \pmod{n^\lambda c}. \text{ —}$$

VII. Seien x, y, $-z$ die drei Wurzeln der Gleichung:

(55) $$x^3 - kx^2 + k_2 x - k_3 = 0, \qquad \text{(L 103)}$$

wobei die Koeffizienten k, k_2, k_3 dargestellt werden durch:

(56) $$\begin{aligned} k &= x + y - z, \text{ grade,} \\ k_2 &= xy - yz - xz, \text{ ungrade,} \\ k_3 &= -xyz, \text{ grade,} \end{aligned} \qquad \text{(L 103, 104)}$$

und setzt man:

(57) $$s_n = x^n + y^n + (-z)^n,$$

so ist bekanntlich:

(58) $$s_n - ks_{n-1} + k_2 s_{n-2} - k_3 s_{n-3} = 0.$$

Wegen (57) und (1) wird dann:

(59) $$-ks_{n-1} + k_2 s_{n-2} - k_3 s_{n-3} = 0.$$

Da nun wiederum:

(60) $$k(s_{n-1} - ks_{n-2} + k_2 s_{n-3} - k_3 s_{n-4}) = 0,$$

so ergeben (59) und (60):

(61)* $$(k_2 - k^2) s_{n-2} + (kk_2 - k_3) s_{n-3} - kk_3 s_{n-4} = 0.$$

LEGENDRE gibt für s_n die WARINGsche Formel:

(62) $$\begin{aligned} s_n = k^n - nk_2 k^{n-2} + nk_3 k^{n-3} + \frac{n(n-3)}{2} k_2^2 k^{n-4} - \frac{n(n-4)}{2} 2k_2 k_3 k^{n-5} \\ + \frac{n(n-5)}{2} k_3^2 k^{n-6} - \frac{n(n-4)(n-5)}{2 \cdot 3} k_2^3 k^{n-6} + \frac{n(n-5)(n-6)}{2 \cdot 3} 3k_2^2 k_3 k^{n-7} \\ - \frac{n(n-6)(n-7)}{2 \cdot 3} 3k_2 k_3^2 k^{n-8} + \frac{n(n-7)(n-8)}{2 \cdot 3} k_3^3 k^{n-9} + \cdots. \end{aligned}$$

MUIR stellt die gleiche Formel unter die Form:

(63) $$s_n = k^n - \sum (-1)^{r+s+t-1} \cdot \frac{n(r+s+t-1)!}{r!\,r!} (-\beta)^r \cdot (\gamma)^s \cdot (\delta)^t, \qquad \text{(L 135)}$$

wobei r, s, t der Bedingung $2r + 3s + 4t = n$ genügen müssen, und β, γ, δ die Ausdrücke

$$\begin{aligned} \beta &= x^2 + xy + y^2 - xz - yz + z^2, \\ \gamma &= x^2 y + xy^2 - x^2 z + xz^2 - y^2 z + yz^2 - 2xyz, \\ \delta &= -xyz(x + y - z) \quad \text{bezeichnen. —} \end{aligned}$$

Sei

(64)* $$x = fn^2 + f', \quad y = gn^2 + g', \quad z = hn^2 + h',$$

so kann man nach (8) setzen:

$$f' + g' - h' = m_1 n^2,$$

und die Gleichung (1) erhält die Form:

(65)* $$(fn^2 + f')^n + (gn^2 + g')^n = [(h - m_1) n^2 + f' + g']^n.$$

Durch Entwicklung dieses Ausdrucks erhält man dann:

(66)* $$(f' + g')^n - f'^n - g'^n \equiv 0 \pmod{n^3}.$$

Wählt man statt (64) die Gleichung (17), so wird:

(67) $$(a^n + b^n)^n - a^{n^2} - b^{n^2} \equiv 0 \pmod{n^{\lambda+1}}.$$ (s. L 160)

Nimmt man jetzt

$$x + y \equiv z \pmod{n^\lambda},$$

so wird durch Potenzieren

$$(x + y)^n \equiv z^n \pmod{n^{\lambda+1}}$$

oder

(68) $$(x + y)^n - x^n - y^n \equiv 0 \pmod{n^3}.$$ (L 6)

Nun ist aber

(69) $$(x + y)^n - x^n - y^n = nxy(x + y)P.$$ (L 20, 23, 114, 129)

Ist dann keine der Zahlen x, y, $z \equiv x + y$ durch n teilbar, so muß P durch n^2 teilbar sein. Kann man nun nachweisen, daß dieses in x und y homogene Polynom P vom Grade $n - 3$ nicht durch n oder gar n^2 teilbar sein kann, so muß der Faktor n^2 in einer der Zahlen x, y, z enthalten sein. (s. L 129)

Der Ausdruck (69) ist besonders von Cauchy, Glaisher, Muir, Catalan untersucht worden. Diese Untersuchungen in ihren Einzelheiten nochmals zu beschreiben, würde hier zu weit führen. Ich gebe daher nur die einschlägigen Resultate an:

(70) $$P \equiv 0 \pmod{x^2 + xy + y^2},$$ (L 23)

und wenn n von der Form $6m + 1$ ist, so ist P sogar durch $(x^2 + xy + y^2)^2$ teilbar. (L 23)

(71) $$Q_r = (x + y)^r + (-x)^r + (-y)^r,$$

(72) $$6 Q_r = 3 Q_2 Q_{r-2} + 2 Q_3 Q_{r-3}.$$ (L 57, 135)

Da

$$xy(x + y) = \tfrac{1}{3}[(x + y)^3 + (-x)^3 + (-y)^3],$$

(73) $$x^2 + xy + y^2 = \tfrac{1}{2}[(x + y)^2 + (-x)^2 + (-y)^2],$$ (L 56, 57, 135)

$$(x^2 + xy + y^2)^2 = \tfrac{1}{2}[(x + y)^4 + (-x)^4 + (-y)^4],$$

so ist Q_n immer durch $Q_2 Q_3$ teilbar, und wenn $n = 6m + 1$ ist, durch Q_4.

(74) $$P = H_1 x^{n-3} + H_2 x^{n-4} y + \cdots + H_1 y^{n-3},$$ (L 19, 20, 21)

$H_r = \frac{1}{n}\left[\binom{n-r}{r} \pm 1\right]$, wobei das Zeichen $+$ bei ungeradem r gilt.

(75)* $$Q_n \equiv 0 \pmod{k}.$$

MUIR gibt für Q_n die Formel: (L 135)

(76) $$(x+y)^{2m+1} - x^{2m+1} - y^{2m+1} = \frac{2m+1}{1}\beta^{m-1}\gamma + \frac{2m+1}{3}\cdot\frac{(m-1)(m-2)}{1\cdot 2}\beta^{m-4}\gamma^3 + \frac{2m+1}{5}\cdot\frac{(m-3)(m-4)(m-5)(m-6)}{1\cdot 2\cdot 3\cdot 4}\beta^{m-7}\gamma^5 + \cdots +,$$

wobei $\beta = x^2 + xy + y^2$ und $\gamma = xy(x+y)$ ist.

Setzt man in (62) z und daher auch k_3 gleich Null, so erhält man $k^n - s_n = Q_n$ unter der Form:

(77) $$Q_n = \sum_{r=1}^{r=\frac{n-1}{2}} (-1)^{r+1}\frac{n}{r}\binom{n-r-1}{r-1}(x+y)^{n-2r} y^r y^r.$$ (L 84, 103, 106, 107, 151, 152)

$(x+y-z) - x^n$ ist durch $z - y$, ebenso $(x+y-z)^n - y^n$ durch $z - x$ und $(x+y-z)^n + z^n$ durch $x+y$ teilbar. Da aber $(x+y-z)^n - x^n - y^n + z^n = (x+y-z)^n$ ist, so muß man die Gleichung aufstellen können:

(78) $$(x+y-z)^n = (x+y)(z-x)(z-y)P_1.$$ (L 19, 25, 94, 95)

Kann man nachweisen, daß $(x+y-z)^n$ nie durch $x+y$, $z-x$ und $z-y$ zugleich teilbar sein kann, so ist dadurch das FERMATsche Theorem bewiesen. —

Ich gebe auch hier wieder nur die Resultate über den Ausdruck

(79) $$(x+y+z)^n - x^n - y^n - z^n:$$

(80) $$\begin{cases}(x+y+z)^n - x^n - y^n - z^n \text{ ist immer teilbar durch} \\ \frac{1}{3}\left[(x+y+z)^3 - x^3 - y^3 - z^3\right].\end{cases}$$ (L 57, 135)

Nehmen wir an $(k = x+y+z)$, es sei:

(81) $$(x+y+z)^n - x^n - y^n - z^n = (x+y)(y+z)(z+x)P_1,$$

so ist:

(82) $$P_1 = k^{n-3} + R_1 k^{n-4} + R_2 k^{n-5} + \cdots + R_{n-3} + y^{n-3} + T_1(x^2, z^2)y^{n-5} + T_2(x^2, z^2)y^{n-7} + \cdots + T_{\frac{n-3}{2}}(x^2, z^2) + x^{n-3} + T_1(y^2, z^2)x^{n-5} + T_2(y^2, z^2)x^{n-7} + \cdots + T_{\frac{n-3}{2}}(y^2, z^2),$$ (L 19)

wobei 1) R_r die Summe aller in x, y, z möglichen Kombinationen von der r^{ten} Dimension darstellt, 2) $T_r(x, z) = x^r + zx^{r-1} + \cdot\cdot + z^{r-1}x + z^r$.

Der entwickelte Ausdruck (79) wird in (62) und (63) durch $k^n - s_n$ dargestellt.

Auf Grund einer ähnlichen Formel findet Herr WENDT, daß:

$$(83)\quad (c^n - b^n - a^n)^n = 2^2 n c^n b^n a^n \sum_{\alpha_1+\beta_1+\gamma_1=\frac{n-3}{2}} \frac{(n-1)!}{(2\alpha_1+1)!\,(2\beta_1+1)!\,(2\gamma_1+1)!} c^{2n\alpha_1} b^{2n\beta_1} a^{2n\gamma_1}. \qquad \text{(L 176)}$$

VIII.* Man betrachte nochmals die Gleichung:

$$(44)\quad z^n - \binom{n}{1} z^{n-1}(a' + b') + \binom{n}{2} z^{n-2}(a'^2 + b'^2) - \cdots - (a'^n + b'^n) = 0.$$

Diese Gleichung hat die Form:

$$(84)\qquad z^n - C_1 z^{n-1} + C_2 z^{n-2} - \cdots - C_n = 0,$$

worin
$$C_r = \binom{n}{r}(a^r + b^r).$$

Setzt man
$$S_r = z_1^r + z_2^r + z_3^r + \cdots + z_n^r,$$

so besteht für jedes $r \geqq 0$ die Kongruenz:

$$(85)^*\qquad S_r \equiv 0 \pmod{n}.$$

Denn alle C_r bis $r = n - 1$ sind durch n teilbar, folglich ist auch:

$$S_1 = C_1 \equiv 0 \qquad \pmod{n}$$
$$S_2 = C_1 S_1 - 2\,C_2 \equiv 0 \quad ,,$$
$$\cdots\cdots\cdots$$

und ebenso $S_n = C_1 S_{n-1} - C_2 S_{n-2} + \cdots + n\,C_n \equiv 0 \pmod{n}$.

Für ein $r > n$ hat man

$$S_r = C_1 S_{r-1} - C_2 S_{r-2} + \cdots \pm S_{r-n} C_n.$$

Alle Glieder der rechten Seite bis auf $S_{r-n} C_n$ sind durch n teilbar. Ist nun $r - n < n$ (d. h. r noch nicht größer als $2\,n$), so ist auch

$$S_{r-n} \equiv 0 \pmod{n},$$

und (85) gilt für alle r von 1 bis $2\,n$. Durch den gleichen Schluß gelangt man dazu, daß (85) auch für alle r von $2\,n$ bis $3\,n$, von $3\,n$ bis $4\,n$ usw., d. h. für alle $r \geqq 0$ Geltung hat. —

IX. Bekanntlich ist immer

$$4\,\varphi(x, y) = X^2 \pm n\,Y^2. \qquad \text{(L 103)}$$

Auf (1) angewandt, wird daraus:

$$(86)\qquad \begin{aligned} 4\,\gamma^n &= X^2 + n\,Y^2, \text{ wenn } n = 4\,m - 1, \\ 4\,\gamma^n &= X^2 - n\,Y^2, \text{ wenn } n = 4\,m + 1. \end{aligned}$$

Im Falle (I) darf X nicht durch n teilbar sein. Im Falle (III) muß n in X enthalten sein, und man hat:

$$4 n \gamma^n = (X_1 n)^2 \pm n Y^2,$$

woraus wieder hervorgeht:

$$4 \gamma^n = n X_1^2 \pm Y^2.$$

Gleiches gilt für $\varphi(z, x)$ und $\varphi(z, y)$. (S. auch *Journ. für Math.* 27, 1844 p. 88 und L 25.) —

X. Multipliziert man jede der Gleichungen (15) entsprechend mit x^n, y^n, z^n und addiert sie, so erhält man:

$$k(x^n + y^n - z^n) = z^n(z - c^n) + x^n(x - a^n) + y^n(y - b^n),$$

und nach (1) ergibt sich:

$$z^{n+1} + x^{n+1} + y^{n+1} = (zc)^n + (xa)^n + (yb)^n. \tag{87} \quad \text{(L 6)}$$

Kann man die Unmöglichkeit einer solchen Gleichung in ganzen positiven Zahlen > 1 nachweisen, so geht daraus auch die Unmöglichkeit von (1) hervor.

Hätte die Gleichung (1) Bestand, und setzte man darin:

$$x^n = x_1, \quad y^n = y_1, \quad z^n = x^n + y^n = x_1 + y_1, \tag{88}$$

so müßte die Gleichung existieren:

$$x_1 y_1 (x_1 + y_1) = z_1^n \tag{89} \quad \text{(L 6)}$$

aus deren Möglichkeit man wiederum Folgerungen auf die Möglichkeit von (1) ziehen kann. —

Nach (1) ist $x = \sqrt[n]{z^n - y^n}$ oder $\frac{x}{z} = \sqrt[n]{1 - \left(\frac{y}{z}\right)^n}$. Es muß daher der Satz bestehen:

(90)* Besitzt $\sqrt[n]{1 - x_1^n}$ keine rationalen Wurzeln, dann hat auch (1) keine ganzzahligen Lösungen und umgekehrt. —

XI. (91)* Ist (1) in ganzen Zahlen unmöglich, dann auch in gebrochenen.

Denn wäre:

$$\left(\frac{x}{x_1}\right)^n + \left(\frac{y}{y_1}\right)^n = \left(\frac{z}{z_1}\right)^n,$$

so wäre auch:

$$(x y_1 z_1)^n + (x_1 y z_1)^n = (x_1 y_1 z)^n. —$$

(92) Ist (1) für einen positiven Exponenten n unmöglich, dann auch für denselben Exponenten mit negativem Vorzeichen. (L 172)

Aus $$x^{-n} + y^{-n} = z^{-n}$$

geht hervor, daß auch:

$$(yz)^n + (xz)^n = (xy)^n. —$$

XII.* Eine der Unbekannten muß, wie schon gesagt, grade und die beiden andern von einer der Formen $4m \pm 1$ sein. Da nun eine Gleichung wie

$$(4\alpha_1 \pm 1)^n + (4\beta_1 \pm 1)^n = (2\gamma_1)^n$$

auf der linken Seite nur durch 2, aber nicht durch 4 teilbar ist, so kann sie nicht bestehen; ebenso $(4\gamma_1 \pm 1)^n - (4\beta_1 \mp 1)^n = (2\alpha_1)^n$. Es sind daher nur folgende Formeln möglich:

$$(93)^* \quad \begin{aligned} (4\alpha_1 + 1)^n + (4\beta_1 - 1)^n &= (2\gamma_1)^n, \\ (4\gamma_1 + 1)^n - (4\beta_1 + 1)^n &= (2\alpha_1)^n, \\ (4\gamma_1 - 1)^n - (4\beta_1 - 1)^n &= (2\alpha_1)^n, \end{aligned}$$

und aus (Ia) folgt, daß z. B. für die erste dieser Gleichungen:

$$(94)^* \quad \alpha_1 + \beta_1 \equiv 0 \pmod{2^{n-2}}.$$

Ebenso sind wegen (27) nur die Formen möglich:

$$(95)^* \quad \begin{cases} (3\alpha_1 + 1)^n + (3\beta_1 - 1)^n = (9\gamma_1)^n, \\ (3\gamma_1 + 1)^n - (3\beta_1 + 1)^n = (9\alpha_1)^n, \\ (3\alpha_1 + 1)^n + (3\beta_1 + 1)^n = (3\gamma_1 - 1)^n, \\ (3\alpha_1 - 1)^n + (3\beta_1 - 1)^n = (3\gamma_1 + 1)^n. \end{cases}$$

Und auch hier ist nach (Ia) für die erste Gleichung:

$$(96)^* \quad \alpha_1 + \beta_1 \equiv 0 \pmod{3^{n-1}}. \text{ —}$$

XIII. (97) Ist m eine beliebige Zahl $\geqq 1$, x' Primzahl, $z' - y' > 1$, so ist die Gleichung $x'^m = z'^n - y'^n$ unmöglich. (s. L 165)

Da $z'^n - y'^n = x'^m$ ist, so muß einer der beiden Faktoren $z' - y'$ und $\varphi(z', y')$ gleich 1 und der andere gleich x'^m sein. Da $\varphi(z', y') = 1$ nicht bestehen kann, so ist nur $z' - y' = 1$ anzunehmen.

Auf gleiche Weise zeigt man:

(98) Ist $m \geqq 1$, z' Primzahl, so ist $z'^m = x'^n + y'^n$ unmöglich. (s. L 165)

Nun ist doch

$$y + z = c^n + b^n, \quad x + z = c^n + a^n, \quad y - x = b^n - a^n.$$

Es folgen daher die Sätze:

(99)* $y + z$ und $x + z$ können nicht gleich einer Primzahl oder gleich der Potenz einer Primzahl sein.

(100)* Ist $b - a > 1$, so kann $y - x$ nicht gleich einer Primzahl oder gleich der Potenz einer Primzahl sein. —

Aus (Ia) kann man direkt den Satz folgern:

(101) Keine der Zahlen $x + y$, $z - y$, $z - x$ kann eine Primzahl sein, mit Ausnahme des Falles $z - y = 1$. — (L 1, 20)

XIV. (102) Die Gleichung

$$x^n \pm y^n = 2^x$$

ist unmöglich für jedes ungrade n. (s. L 9)

Da x und y als relativ prim anzusehen sind, so müssen sie ungrade sein, und $x \pm y$ ist eine grade Zahl. $\varphi(x, y)$ ist aber ungrade. Nun kann doch nicht eine ungrade Zahl Teiler einer Potenz 2^x sein, wenn nicht $\varphi(x, y) = 1$, was ausgeschlossen ist, denn es kann nicht $x^n \pm y^n = x \pm y$ sein. —

(103)* Die Gleichung

$$x^n \pm y^n = n^{n\lambda}$$

ist unmöglich.

Sei

$$x^n + y^n = n^{n\lambda},$$

so hat man nach (IIId), wobei $z = n^\lambda$ ist:

$$2z = 2n^\lambda = n^{n\lambda - 1} + b^n + a^n;$$

es müßte also

$$2n^\lambda > n^{n\lambda - 1}$$

sein, was für jedes λ unmöglich ist, wenn $n \geqq 3$.

Ebenso hat man für $z^n - y^n = n^{\lambda n}$:

$$2n^\lambda = c^n - b^n + n^{n\lambda - 1},$$

worin $c^n - b^n$ positiv ist und man denselben Schluß wie oben ziehen kann.

Aus diesen Beweisen resultiert auch der Satz:

(104)* Keine der Zahlen $x + y$, $z - y$, $z - x$ kann eine Potenz von n sein. —

XV. (105). Ist $y > x$, so kann weder y noch z eine Primzahl oder die Potenz einer Primzahl sein. (s. L 1, 20, 21, 45, 69, 70, 126)

Angenommen, y sei eine Primzahl, so muß, wie bei (97), $z - x = 1$ sein, was aber nicht zutreffen kann, da $z > y > x$, der Unterschied zwischen z und x also mindestens 2 sein muß.

Sei nun z eine Primzahl, so gelangt man durch den bei (97) angewandten Schluß zu der unmöglichen Relation $x + y = 1$.

Nehmen wir jetzt an, x sei eine Primzahl, so gelangen wir wie bei y zu der Relation:

(106a) $$z - y = 1.$$ (L 20, 21, 69, 70)

Unter Berücksichtigung von (8), (16), (27) erhält man dann:

(106b)* $$x \equiv 1 \pmod{9cbn^2}.$$

Ähnliches folgt aus (69) und (70), denn:

(106c) $$x^n - 1 = (y + 1)^n - y^n - 1^n \equiv 0 \pmod{nzy(y^2 + y + 1)}. —$$ (L 20)

(106d) Jeder Primfaktor von $z - x$ ist es auch von $x - 1$. (L 20)

Denn sei

$$y^n = (y+1)^n - x^n = (y + 1 - x)E,$$

so muß jeder Primfaktor von $y + 1 - x$ auch ein solcher von y^n oder vielmehr von y sein, d. h. auch von $y - (y + 1 - x) = x - 1$. (106d) geht auch aus (Ia) und (106b) hervor. —

(106e) $2x - 1$ und $2y + 1$ haben keinen gemeinschaftlichen Faktor. (L 20)

Denn $x + y$ und $y + 1 - x$ sind relativ prim und daher auch ihre Summe und Differenz untereinander. —

Aus der Potenzentwickelung von

$$x^n = (y+1)^n - y^n$$

findet man:

$$\sqrt[n]{n(y+1)^{n-1}} > x > \sqrt[n]{n y^{n-1}},$$

(106f)
$$\left(x\sqrt[n-1]{\frac{x}{n}}\right) > y > \left(-1 + x\sqrt[n-1]{\frac{x}{n}}\right),$$
(L 20)

wodurch sich x und y auseinander ziemlich genau bestimmen. —

XVI.*(107)* Die Gleichung $x^n + y^n = (y+2)^n$ ist in teilerfremden Zahlen x, y, $y + 2$ unmöglich.

y und $y + 2$ müssen ungrade und x grade sein. Man kann deshalb setzen:

$$(2x_1)^n + y^n = (y+2)^n,$$

oder

$$2^n x_1^n = n y^{n-1} \cdot 2 + \binom{n}{2} y^{n-2} \cdot 2^2 + \cdots + 2^n.$$

Alle Glieder bis auf das erste der rechten Seite enthalten den Faktor 2^2. Da aber $2ny^{n-1}$ nicht durch 4 teilbar sein kann, so kann die Gleichung (107) nicht bestehen. — Der Satz (107) geht auch direkt aus (Ia) hervor, und man kann für numerische Bestimmungen (Ia) in der Form ausdrücken, daß in $x^n + y^n = (y + a')^n$ die Zahl a' nicht gleich 3, 4, 5 usw., überhaupt keine Zahl sein kann, die nicht eine n^{te} Potenz ist. — (107) gilt natürlich nicht, wenn x, y, z einen gemeinschaftlichen Teiler haben. Herr Umfahrer glaubt z. B. (L 171), daß der Satz (107) auch für $(2x)^n + (2y)^n = (2y + 2)^n$ gilt, was aber hieraus nicht bewiesen werden kann. —

(108)* Die Gleichung $x^n + (x + su)^n = (x + tu)^n$ ist unmöglich.

Wäre diese Gleichung möglich, so hätten $z - y = u(t - s)$ und $z - x = tu$ einen gemeinschaftlichen Faktor, was bei teilerfremden x, y, z mit Ausnahme von $u = 1$ ausgeschlossen ist. Haben aber x, y, z einen gemeinschaftlichen Teiler, so ergeben sie, durch diesen gekürzt, wieder eine Gleichung von der

Form (108) mit relativ primen Unbekannten.[1]) — Der Satz (108) kann auch in der Form ausgesprochen werden:

(109)* Außer der natürlichen Zahlenreihe ($u = 1$) gibt es keine arithmetische Progression, in der drei beliebige Glieder der Gleichung (1) genügen.

Kann man nun nachweisen, daß die drei Zahlen x, y, z Glieder einer arithmetischen Progression mit der Differenz $u > 1$ sein müssen, so ist nach (109) die Unmöglichkeit von (1) erwiesen.

2. Geschichtliche Übersicht.

Der erste bekannte Versuch, das Fermatsche Theorem allgemein zu behandeln, ist in einem Manuskript der Pariser Bibliothek enthalten, das man erst Malebranche zuschrieb (s. L. 61), dann aber als eine Arbeit Claude Jaquemets (1651—1729) erkannte. Die kleine Schrift (L 68) ist insofern bemerkenswert, als darin zum erstenmal der Satz (2) aufgestellt und bewiesen wird, zu dessen Beweis man später die Waringsche Formel benutzte. Wäre der Verfasser einen Schritt weiter gegangen, so hätte er schon die wichtigen Formeln (I)—(III) erhalten, die erst anderthalb Jahrhunderte später aufgestellt wurden. Bei diesen Formeln ist es eine merkwürdige Tatsache, daß die meisten ihrer Aufsteller sie unabhängig voneinander gefunden haben (Abel, Barlow, Kummer für $n = 2\lambda$, Legendre, Lindemann, F. Lucas, Stäckel). Der erste von ihnen ist Barlow. Er gibt in seiner „Theory of Numbers" (L 5) einen Beweis, der an der Annahme scheitert, daß $\frac{t^{n-1}}{sr} - \frac{s^{n-1}}{tr} - \frac{r^{n-1}}{st}$ keine ganze Zahl sein könne, wenn r, s, t relativ prim sind (siehe L 166). Daß in diesem Beweise die Formeln (I)—(III) und (16) enthalten sind, ist wohl den wenigsten bekannt gewesen, denn die meisten gingen von Legendres oder Abels grundlegenden Arbeiten aus. Legendre hat eine große Zahl der in I., II. und VII. aufgeführten Formeln gefunden und sie mit ihren Beweisen in L 103 veröffentlicht. Abel teilt in seinem Briefe an Holmboe am 24. Juni 1823 (L 1) ohne Beweise die Formeln (I)—(III) und verschiedene andere Sätze mit, die später zum größten Teil bewiesen worden sind, zum Teil heute noch offen stehen, zum kleinen Teil aber unrichtig sind. — Herr Lindemann bezeichnet in der Berichtigung seines ersten Beweises (L 106), bei dem er die Abelschen Formeln (I)—(III) herleitet, die Arbeit insofern als einen Fortschritt, als diese Formeln darin zum erstenmal bewiesen worden seien. Ebenso beweist Herr Stäckel 1903 (L 159) zum hundertsten Geburts-

[1]) Natürlich gilt dies nicht, wenn nach der Kürzung drei Zahlen entstehen, die nur in der natürlichen Zahlenreihe vorkommen, und das kann nur der Fall sein, wenn x, y, z durch u teilbar sind.

tage ABELS nochmals diese Formeln, obwohl dieselben fast 100 Jahre vorher, 12 Jahre vor den ABELschen Untersuchungen festgestellt worden sind. — F. LUCAS zeigt in L 114 die Herleitung der Formeln (Ia)—(IIIa) mit Hilfe des Satzes über die Teilbarkeit des Ausdrucks $(x + y)^n - x^n - y^n$. Es mögen hier noch die beiden Versuche RIEKES erwähnt werden, in denen ebenfalls die ABELschen Formeln und einige bemerkenswerte Kongruenzen hergeleitet werden, die aber beide mit unüberbrückbaren Fehlern behaftet sind. — Aus (1) erhält Herr WENDT in L 176 etwas allgemeiner scheinende Formeln, die aber dieselben wie die in I. angegebenen sind. Nach der bei JAQUEMET angewandten Methode leitet 1901 T. R. BENDZ in seiner Dissertation (L 6) die ABELschen Formeln her, sowie verschiedene andere in I.—IV. und X. gefundene Formeln, von denen ich besonders die Kongruenz (26) erwähne, da ich durch dieselbe veranlaßt wurde, die Kongruenzen (27)—(31) aufzustellen. Ferner wird darin der Satz ausgesprochen: „Die notwendige und hinreichende Bedingung, daß die Gleichung $x_1^n + y_1^n = z_1^n$ eine ganzzahlige Lösung besitze, ist die, daß die Gleichung $\alpha^2 = 4\beta^n + 1$ eine rationale Lösung habe und umgekehrt", der leicht aus der Gleichung $\left(\frac{2y^n + x^n}{x^n}\right)^2 = 4\left(\frac{yz}{x^2}\right)^n + 1$ hergeleitet werden kann (vgl. IX.). — In der schon erwähnten Abhandlung des Herrn LINDEMANN findet dieser eine Identität, die aber dieselbe wie die in (77) gegebene WARINGsche Formel ist, die wir schon in fast derselben Form an analoger Stelle bei L 151 sahen. Diese Identität, aus der Herr LINDEMANN z. B. die Kongruenzen (19) modulo n ableitet, findet sich bei KUMMER in L 84, sowie schon bei GRUSON (Abh. Ak. Berlin 1813—15). Auch läßt sie sich, wie in (77) gezeigt worden ist, aus der bei LEGENDRE aufgestellten Formel ableiten. LEGENDRE entwickelte dabei die Summe der n^{ten} Wurzelpotenzen der Gleichung $x^3 - kx^2 + k_2x - k_3 = 0$, wie ich dies in (62) dargestellt habe, wobei k, k_2 und k_3 die in (56) angegebenen Werte besitzen. In seiner Zahlentheorie, Art. 451 (deutsche Ausg. p. 118—120), bemerkte er noch einige Eigenschaften dieser drei Größen und behauptete dabei, daß ebenso wie $k = x + y - z$ auch $k_3 = -xyz$ durch n^2 teilbar sei. Diese Bemerkung ist zu korrigieren, da es nicht allgemein erwiesen war, daß eine der Unbekannten durch n teilbar sein muß.[1])

Von den andern Sätzen, die ABEL aufgestellt hat, ist wohl der der wichtigste, daß keine der Größen x, y, z, $x + y$, $z - y$ usw. eine Primzahl sein könne. Wieder war es ein Engländer, TALBOT, der 1857 in L 165 die Formeln (97), (98)[2]), (105) und (106a) zum erstenmal bewies, von Späteren aber kaum berücksichtigt wurde. JONQUIÈRES führte 1884 in L 69 unabhängig von ihm

---

[1]) siehe Nachtrag.

[2]) (97) und (98) bewies TALBOT nur für $m < n$ mittels eines andern als bei (97) angegebenen Beweises.

einen ähnlichen Beweis. In C. R. 1884 (L 70) berichtete er über diese Abhandlung mit dem Hinweis auf ABELS Satz, der bis dahin noch nicht bewiesen worden wäre. Im Anschluß an diese (105) und (106a) enthaltende Untersuchungen gab CATALAN 1866 (L 20) die Sätze (22), (23), (101), (105)—(106f), die er nochmals in L 21 zusammenfaßte. Ein Jahr später versuchte Herr MANSION (L 126) außer dem Unmöglichkeitsbeweis für die beiden größeren Unbekannten als Primzahlen auch den für die kleinste; der letzte Beweis war jedoch falsch, was der Verfasser auch S. 225 berichtigte. Bei diesem Beweise erhielt Herr MANSION die Formel (47) und bemerkte zu der Gleichung $z = a_1 x + b_1 y$, daß er aus dieser für das Studium des FERMATschen Theorems sehr wichtigen Gleichung eine Menge Konsequenzen abgeleitet habe, die er später zu veröffentlichen gedenke. Es ist jedoch meines Wissens keine solche Arbeit von Herrn MANSION erschienen. Im gleichen Jahre bewies nochmals BORLETTI (L 9), daß in der Gleichung (1) z keine Primzahl sein könne, daß in der Gleichung $x^{2n} - y^{2n} = z^{2n}$ keine der Unbekannten eine Primzahl sein könne, sowie die Unmöglichkeit der Gleichung $x^n \pm y^n = 2^{\alpha n}$ (s. (102)). — In einer bibliographischen Arbeit (L 45), in der verschiedene Sätze und Memoiren über das letzte FERMATsche Theorem zusammengefaßt werden, zeigt D. GAMBIOLI die Unmöglichkeitsbeweise für die Primzahlen x, y, z; jedoch ist hier wiederum der Beweis für die kleinste der Unbekannten mißglückt. Noch im Jahre 1905 beweist R. SAUER in seiner Dissertation (L 155), die auch in ihren anderen Teilen nichts Neues enthält, daß die Summe der n^{ten} Potenzen zweier Primzahlen usw. nicht gleich einer n^{ten} Potenz sein könne.

Bei dem Bericht über den LAMÉschen Beweis des Falles $n = 7$ bemerkt CAUCHY (L 23), daß der Ausdruck $(x+y)^n - x^n - y^n$ immer durch $nxy(x+y)(x^2+xy+y^2)$ teilbar ist, und wenn $n = 6m+1$, sogar durch $(x^2+xy+y^2)^2$ (s. VII.). Von welcher Bedeutung die Untersuchung dieses Polynoms ist, zeigt die nach (69) bemerkte Beweismöglichkeit, die von MATHEWS (L 129) ausgesprochen wurde, oder der bereits erwähnte Aufsatz von F. LUCAS (L 114).[1]) GLAISHER, MUIR, MAC MAHON, BINI leiten verschiedene Sätze für den bezeichneten Ausdruck ab, von denen ich einige in VII. wiederholt habe. CATALAN (L 20) macht von CAUCHYS Satz Anwendung auf den Fall, daß x eine Primzahl sei, und erhält die in (106c) angegebenen Resultate. Auch die Untersuchungen über den Ausdruck $(x+y+z)^n - x^n - y^n - z^n$, die in engen Beziehungen zu den eben genannten stehen, hat CATALAN durch schöne Sätze gefördert (L 19).

In seiner ersten Arbeit über den FERMATschen Satz (L 84) behandelt KUMMER den Fall eines graden Exponenten und entwickelt darin verschiedene

[1]) siehe auch Nachtrag.

den (I) — (III) analoge Formeln, die wohl nur historischen Wert besitzen, da es ja genügt, den Exponenten als Primzahl anzunehmen. Im fünften Bande des Journ. de Math. beweist LEBESGUE (L 98) den Satz: „Ist die Gleichung $x^n + y^n = z^n$ unmöglich, so ist es auch die Gleichung $X^{2n} + Y^{2n} = Z^{2}$"; und LIOUVILLE (L 108) zeigt in demselben Bande, daß unter der gleichen Annahme die Gleichung $Z^{2n} - Y^{2n} = 2X^n$ ebenfalls unmöglich ist. — GRUNERT erhält in L 59 auf nahezu einer Seite das Resultat, daß (1) in positiven ganzen Zahlen $< n$ unmöglich ist. Ich verweise hier auf die Gleichung (33), aus welcher direkt folgt, daß die Unbekannten $> 54\,n^2$ sein müssen. — In (108) habe ich die Gleichung $x^n + (x + su)^n = (x + tu)^n$ als unmöglich erwiesen. Für $s = 1$ und $t = 2$ zeigten die Herren BOTTARI (L 10) und CATTANEO (L 22) die Unmöglichkeit, d. h. daß die Größen x, y, z nicht aufeinanderfolgende Glieder einer arithmetischen Progression sein können, und zwar auf Grund des Beweises, daß x, y, z nicht drei aufeinanderfolgende Zahlen sein können. Der letzte Satz, der besonders bei Herrn BOTTARI ziemlich umständlich behandelt wird, folgt direkt aus (107).

Im Interméd. des Math. (L 179) stellt Herr WORMS DE ROMILLY ohne Beweisangabe die Formeln auf:

$$z = c' + b' + a', \quad y = c' + b', \quad x = c' + a',$$

$$c' = M\frac{n^{n(\nu+1)-1} + a^{n(\nu+1)-1}}{2} n^{\nu+1} q^{\nu+1}, \quad b' = q^{n(\mu+1)}, \quad a' = n^{n(\nu+1)}.$$

Hätte Herr WORMS DE ROMILLY, wie er behauptet, einen Beweis für diese Formeln, so wäre dies auch ein Beweis des FERMATschen Theorems, denn nach (104) kann $z - y = a'$ keine Potenz von n sein. Im Grunde sind diese Formeln dieselben, wie die in (II) gegebenen (vgl. (43)). Und mit Hilfe der letztgenannten sucht Herr WEREBRUSOW 1908 die Frage W. DE ROMILLYS zu beantworten, ob nämlich der Beweis des FERMATschen Satzes mittels dieser Formeln dekannt sei. Jedoch enthält der Beweis WEREBRUSOWS einen Fehler der p. 174—177 von verschiedenen Lesern berichtigt wird. Herr W. DE ROMILLY, der sich auch unter den Berichtigern befindet, nennt nochmals die Formeln (I)—(III) und am Schluß die folgenden:

$$x = \tfrac{1}{2}(n^{n\lambda} - n^{n\lambda} g^n + f^n), \quad y = \tfrac{1}{2}(n^{n\lambda} + n^{n\lambda} g^n - f^n), \quad z = \tfrac{1}{2}(n^{n\lambda} + n^{n\lambda} g^n + f^n),$$

die aber nicht bestehen können, da $x + y$, $z - x$, $z + y$ den gemeinschaftlichen Faktor $n^{n\lambda}$ enthalten.

Ich will hier noch auf die Fehler einiger allgemeiner „Beweise" eingehen, von denen ich keine Berichtigung gelesen habe: PAULET erhielt in (L 137): $[bmx^2 - (p - q)a]\,cr = [ar + (p - q)\,c + s]s$, woraus er den unberechtigten Schluß zog, daß der erste Faktor des linken Gliedes gleich dem ersten des rechten und der zweite des linken Gliedes gleich dem entsprechenden auf der

andern Seite sein müßte. Beim zweiten Beweis wurden dadurch willkürliche Werte angenommen, daß der Verfasser verschiedene Summanden gleicher Summen einander gleichsetzte. Die andere Arbeit (L 138) ist in dem gleichen Band berichtigt. — In der Abhandlung CALZOLARIS (L 15), die von GAMBIOLI in sein Memoria bibliografia aufgenommen worden ist, beging ersterer den Fehler, daß er annahm, wenn eine grade Zahl in dem Produkt einer ungraden und einer graden enthalten sein mußte, daß diese Zahl vollständiger Faktor des graden Teilers sein müßte. — (L 156): SCHIER glaubte, wenn der Faktor n^2 in $(x + y)^n - x^n - y^n$ enthalten war, so müßte er in $nxy(x + y)$ enthalten sein, was der Verfasser nur in etwas anderer Weise aussprach. Im Falle, daß x durch n teilbar ist, übersah SCHIER, daß $z - y$ den Faktor n in der $(n - 1)^{\text{ten}}$ Potenz enthalten mußte. — (L 48): Der Unmöglichkeitsbeweis von (1) wird einmal daraus geschlossen, daß die linke Seite eine andere Zerlegungsart als die rechte besitze. Die beiden andern Gründe enthalten überhaupt keine Konsequenz.

In Bezug auf die neuere Fehler-Literatur verweise ich auf L 44. Von den dort nicht genannten Schriften sind mir folgende zu Händen gekommen: L 7: Autor nimmt für $x + y$, $y - x$, usw. unberechtigte willkürliche Werte an, für die wohl die FERMATsche Gleichung unmöglich sein kann, aber nicht allgemein. Setzt man z. B. allgemein $y - x = 2b$, so sieht man, daß nur bei ganz bestimmten a und b die Möglichkeit $y + 1 > z$ eintreten kann. — L 62: Der Grund dafür, daß $\frac{c^n}{c + w}$ ein Bruch sein muß, ist vollständig unhaltbar. Wenn $\frac{c + w}{c}$ und $\frac{c + w}{c^n}$ Brüche sind, so folgt daraus noch nicht, daß $\left(\frac{c}{c + w}\right) c^n$ ebenfalls ein Bruch sein muß. — L 66: Der Verfasser schließt aus der Teilbarkeit von y^m durch $z - x = \alpha$, daß α auch in y enthalten sein müsse. — L 131: Die Summe von zwei irrationalen Zahlen muß nicht „selbstverständlich" ebenfalls irrational sein. Übrigens gibt die CARDANsche Formel oft ganzzahlige Unbekannten in irrationaler Form. Dasselbe ist bei $n = 4$ zu sagen. Für höhere Potenzen beruft sich der Verfasser darauf, daß ABEL bewiesen hat, daß eine direkte Berechnung der Unbekannten nicht möglich ist. Wenn die Berechnung der Gleichungswurzeln unmöglich ist, so ist noch nicht die Gleichung in ganzen Zahlen unmöglich. — Zu L 181 ist zu bemerken: Der Verfasser, in dessen Inkognito übrigens die einzige Konsequenz liegt, läßt nach unerlaubten Voraussetzungen unzusammenhängende Theoreme und falsche Gleichungen aufeinanderfolgen, deren Berichtigung vielleicht die zwölf Seiten in Anspruch nehmen könnte, die der anonyme Verfasser zu seinem Beweise nötig hat. —

Für den ersten speziellen Beweis seines berühmtesten Satzes hatte FERMAT selbst ein Verfahren im Falle $n = 4$ angegeben, das von EULER zum Beweis

der Unmöglichkeit von $x^4 \pm y^4 = z^2$ angenommen wurde (L 38). 22 Jahre später fügte der große Baseler Mathematiker diesem noch den scharfsinnigen Beweis für $n = 3$ hinzu (L 40), der genauer in seiner Algebra behandelt ward. Vergebens suchte EULRR, der ja viele Sätze FERMATS bewiesen hatte, das letzte FERMATsche Theorem allgemein zu zeigen. Es gelang ihm nicht; aber er hatte dabei Gelegenheit gehabt, über die Teilbarkeit von Potenzbinomen eingehende Studien zu machen, deren schöne Resultate sich in L 39 und L 42 finden. KAUSLER zeigte nochmals die Unmöglichkeit der FERMATschen Gleichung für $n = 3, 4, 6$ (L 73—75), BARLOW für $n = 3, 4$ (L 5) und LEGENDRE für den ersteren Fall mittels einer neuen eleganten Beweismethode. Da erschien 1825 die erste Arbeit des jungen DIRICHLET (L 33), in der er zeigte, daß im Falle der fünften Potenz eine der Unbekannten durch 5 teilbar sein müsse und daß diese nicht ungrade sein könne. LEGENDRE, der sich lebhaft für die schöne Beweisart interessierte, erwies mittels derselben Methode, daß die durch 5 teilbare Zahl auch nicht grade sein könne. Den jetzt vollständigen Beweis der Unmöglichkeit der Gleichung $x^5 + y^5 = z^5$ in ganzen Zahlen, der auch in seine „Theorie des nombres" aufgenommen wurde (L 104), gab LEGENDRE zusammen mit seinen übrigen Untersuchungen über den FERMATschen Satz in L 103 heraus. Bei diesen zeigte der große Zahlentheoretiker u. a., daß für den Fall $n = 7$ eine der Unbekannten durch 7 teilbar sein müsse. Für $n = 2 \cdot 7$ erwies DIRICHLET 1832 (L 34) die Unmöglichkeit der FERMATschen Gleichung. 1840 zeigte LAMÉ, daß der Satz auch Gültigkeit für die siebente Potenz habe, und daher auch für den von DIRICHLET bewiesenen Fall. LEBESGUE wurde durch den LAMÉschen Beweis angeregt und zeigte noch in demselben Jahre im gleichen Band von Liouv. Journ. einen neuen vereinfachten Beweis für $n = 7$. — Es sind dies die wichtigsten ersten Beweise für einen speziellen Exponenten. Die späteren meistens gleiche Fälle betreffenden Essays kann ich hier nicht einzeln behandeln. Es sind dies vorzüglich folgende:

$n = 3$: CALZOLARI 1865 (L 15); LAMÉ 1865 (L 96); PEPIN 1870 (L 140), 1881 (L 143); TAIT 1872 (L 164); BROCARD 1878 (L 14); GÜNTHER 1878 (L 60); RÉALIS 1878 (L 150); E. LUCAS 1878 (L 111), 1880 (L 112); PERRIN 1884 (L 146); GAMBIOLI 1901 (L 45);

$n = 4$: LEBESGUE 1853 (L 101); PEPIN 1883 (L 145); TAFELMACHER 1893 (L 161); GAMBIOLI 1901 (L 45); BENDZ 1902 (L 6); BANG 1905 (L 3);

$n = 5$: LEBESGUE 1843 (L 100); LAMÉ 1847 (L 93); WEREBRUSOW 1905 (L 177);

$n = 6$: TAFELMACHER 1897 (L 162);

$n = 7$: LAMÉ 1843 (L 92); GENOCCHI 1864 (L 51), 1876 (L 52); PEPIN 1876 (L 141); MAILLET 1897 (L 117), 1901 (L 119);

$n = 37$: MIRIMANOFF 1897 (L 132).

An dieser Stelle möge auch L 158 erwähnt werden, da hier nochmals die Beweise FERMATS, LEGENDRES, KUMMERS usw. dargestellt werden. Ebenso die Arbeit des Herrn TAFELMACHER über das letzte FERMATsche Theorem (L 160), in der er (I)—(III), sowie einen Teil der in II. gefundenen Formeln aufstellt. Im zweiten Teil dieser Abhandlung beweist er dann die allgemeine Unmöglichkeit von (1) für $n = 3, 5, 11, 17, 23, 29$, und im Falle $k \equiv 0 \pmod{n^4}$ für $n = 7, 13, 19, 31$. Allein diese Beweise werden wohl nur für nicht durch n teilbare Zahlen x, y, z gelten müssen, denn Herr TAFELMACHER erwägt diesen Fall nicht besonders, und die Schlüsse auf p. 273—278 berechtigen noch nicht, auszuschließen, daß eine dieser Zahlen durch n teilbar sei. —

Im handschriftlichen Nachlaß von GAUSS befindet sich ein Artikel zur Theorie der komplexen Zahlen (L 49). Darin wird für einzelne Fälle der FERMATschen Gleichung bewiesen, daß eine der Unbekannten durch den Exponenten teilbar sein müsse. In ähnlicher Weise zeigt dies LEGENDRE in L 103. Daran anschließend zeigt er mittels eines Verfahrens, das von SOPHIE GERMAIN stammt, daß für alle $n < 100$ eine der Unbekannten durch n teilbar sein muß. Im Anfang seiner Abhandlung sagt LEGENDRE, daß die Bedingung, so leicht sie für kleine Exponenten zu erweisen sei, zu einem schweren Problem werde, wenn man sie auf jeden Exponenten ausdehnen wolle. BOUNIAKOWSKY gibt 1831 (L 12) eine der GERMAIN-LEGENDREschen ähnliche Methode, mittels der diese Bedingung bis zu $n = 29$ als erfüllt gezeigt wird. — Herr WENDT gelangt in L 176 zu verschiedenen Kriterien für die Teilbarkeit der Unbekannten durch n, die für einen allgemeinen Beweis zwar keine Bedeutung besitzen, durch die es aber Herrn MIRIMANOFF (L 133) ermöglicht wurde, im Anschluß an die schönen MAILLETschen Untersuchungen ($n < 223$) die von LEGENDRE gestellte Bedingung bis auf $n < 257$ auszudehnen. Aber alle diese Untersuchungen sind weit übertroffen worden von den eingehenden Arbeiten des Herrn DICKSON. Derselbe gelangt in L 30, p. 44 zu dem Ergebnis: „Die FERMATsche Gleichung $u^n + v^n = w^n$ ist unmöglich in ganzen zu n primen Zahlen für jede ungrade Primzahl $n < 6857$ und für die größeren < 7000."[1]) —

Von allen Untersuchungen sind die KUMMERschen die erfolgreichsten auf dem Gebiete des FERMATschen Problems gewesen. Es war das an hervorragenden Arbeiten über den großen FERMATschen Satz so reiche Jahr 1847. LAMÉ hatte versucht, in L 93 die Unmöglichkeit der Gleichung (1) in komplexen Zahlen für den Fall $n = 5$ und endlich in L 94 für den allgemeinen Fall zu erweisen. Jedoch konnten diese unter falschen Voraussetzungen (s. L 109) durchgeführten Beweise das FERMATsche Theorem direkt in keiner Weise fördern. Aber indirekt hatten sie insofern einen Nutzen, als CAUCHY durch

[1]) vgl. Satz (110) im Nachtrag.

die Arbeiten LAMÉs zu den großzügigen Untersuchungen angeregt wurde, die sich in L 25—26 finden. Und auch diese Untersuchungen fanden keine praktische Anwendung auf einen speziellen oder allgemeinen Beweis. Erst KUMMER (L 86) gelang es, mit Hilfe der Theorie der Primideale zu zeigen, daß die Gleichung (1) in ganzen Zahlen unmöglich sei für alle diejenigen Exponenten n, welche ungrade Primzahlen sind und in den Zählern der ersten $\frac{n-3}{2}$ BERNOULLIschen Zahlen als Faktoren nicht vorkommen. Zu diesen Exponenten gehören alle ungraden Primzahlen < 100 außer 37, 59 und 67. Zehn Jahre später zeigte der hervorragende Mathematiker, daß die Gleichung (1) noch für eine weitere Reihe von Exponenten unmöglich sei (L 88), zu denen auch die drei genannten gehören, so daß die FERMATsche Behauptung für alle Exponenten > 2 und $\leqq 100$ erwiesen war. Die verschiedenen 1847er Arbeiten hatten der Pariser Akademie Anlaß gegeben (s. L 182), das FERMATsche Problem 1850 zum Gegenstand des großen Preisausschreibens zu wählen. Da der bis 1856 verlängerte Wettbewerb ohne einen weitergehenden Erfolg verlief, wurde der Preis KUMMER für seine schönen Untersuchungen zuerteilt. — Nach den letztgenannten Abhandlungen KUMMERS ruhten die Arbeiten über die Theorie der komplexen Zahlen in ihrer Anwendung auf den großen FERMATschen Satz eine lange Zeit. Herr HILBERT faßte in seiner „Theorie der algebraischen Zahlkörper" nochmals die KUMMERschen Resultate vereinfacht und verbessert zusammen (L 64). Von den späteren Schriften auf diesem Gebiete sind noch zu nennen die Arbeiten von MATHEWS (L 130), THUE (L 169), MAILLET (L 117—123), BENDZ (L 6), MIRIMANOFF (L 133), DICKSON (L 28—32). —

Im vorangegangenen habe ich, so gut es mir möglich war, alle Wege gezeigt, die bei einem Beweise des letzten FERMATschen Theorems eingeschlagen worden sind. Fast alle sind sie bis zur Hälfte durchlaufen worden, aber kaum einer darüber hinaus. Ich hoffe, daß meine Ausführungen anregende Gelegenheit bieten, einen dieser Wege weiterzuführen und es zu ermöglichen, den in der Mitte des siebzehnten Jahrhunderts ausgesprochenen Satz im zwanzigsten Jahrhundert in seiner vollen Ausdehnung als richtig erkennen zu lassen. Solche Erzeugnisse natürlich, wie die neuen Fehlerbeweise, wobei jeder allein ohne Berücksichtigung der gründlichen Arbeiten großer Mathematiker blind auf das Ziel losstürzend es zu erreichen glaubt, können uns das Ziel, den Fortschritt der Wissenschaft (nicht die Erlangung von 100000 Mk.!), nicht näher bringen.

3. Literaturverzeichnis.

[1] Abel, Hendrik. „Extraits de quelques lettres à Holmboe". Werke II. p. 254—255.

[2] Ball, W. W. Rouse. Mathematical recreations and problems. London 1892, p. 27—30 (Fermat's last theorem). Franz. von Fitz-Patrick. Paris 1907—08.

[3] Bang, Aage. „Nyt Bevis for at Ligningen $x^4 - y^4 = z^4$ ikke kan have rationale Lösninger". Nyt Tidsskr. f. mat. 16. 1905 p. 35—36.

[4] Barlow, Peter. „Demonstration of a curious numerical proposition". Nichols. Journ. 27. 1810. p. 193—205.

[5] —— Theory of numbers. London 1811. p. 132—140 ($n = 3$); p. 118—122, 144—145 ($n = 4$); p. 160—169 (n allgemein). (Berichtigung siehe L 166.)

[6] Bendz, Torsten Ragnar. „Öfver diofantiska ekvationen $x^n + y^n = z^n$". Dissert. Upsala 1901. (34 S.) Lundequistska bokhandeln 1902.

[7] Best, Ludwig. „Beweis des Fermatschen Satzes". Darmstadt 1908 (H. L. Schlapp).

[8] Bini, Umberto. „Sopra alcune congruenze". Per. di Math. 22 (ser. 3) IV. 1907. p. 180—183.

[9] Borletti, F. „Sopra il teorema di Fermat relativo all' equazione $x^n + y^n = z^n$". Reale Ist. Lomb. Rendiconti (2) XX. 1887. p. 222—224.

[10] Bottari, Amerigo. „Soluzione intere in progressione aritmetica appartenenti a equazione indeterminate de tipo $\sum_{\nu=1}^{r} x_\nu^n = x_{r+1}$". Per. di Math. 22 (3) IV. 1907, p. 156—168.

[11] —— „Soluzione intere dell'equazione pitagorica e applicazione alle dimostrazione di alcune teoremi della teori dei numeri". Per. di Math. 23. (3) V. 1908, p. 104—110.

[12] Bouniakowsky, V. „Recherches numériques". Mém. Ac. St.-Petersb. (6) I. 1831, p. 139—152.

[13] —— „Notes sur quelques points de l'analyse indéterminée". Bull. Ac. St.-Petersb. VI. 1848, p. 200—201.

[14] Brocard, H. „Notes sur divers articles . . . . ". Nouv. Corr. Math. IV. 1878, p. 136—138.

[15] Calzolari, Luigi. „Tentativo per dimostrare il teorema di Fermat sull' equazione indeterminata $x^n + y^n = z^n$". Ferrara 1855 = L 45, p. 153.

[16] —— „Dimostrazione dell' ultimo teorema di Fermat". Annali di sc. mat. VIII. 1857, p. 339—349.

[17] —— „Impossibilita in numeri interi dell' equazione $z^n = x^n + y^n$ quando $n > 2$". Annali di Mat. VI 1864, p. 280—286.

[18] Catalan, Eugène. „Rapport" (über den Wettbewerb) (s. L 125, 170). Bull. Ac. Belg. 52 (3) VI. p. 814—819.

[19] —— „Sur le théorème de Fermat" = Mélanges Mathématiques 47. Mém. Soc. Liège (2) XII. 1885, p. 179—185.

[20] —— „Sur le dernier théorème de Fermat" = Mél. Math. 215. Mém. Soc. Liège (2) XIII. 1886, p. 387—397.

[21] —— „Sur le dernier théorème de Fermat". Bull. Ac. Belg. (3) XII. 1886, p. 498 —500.

[22] Cattaneo, Paolo. „Osservazione sopra due articoli del signor Amerigo Bottari". Per. di Math. 23. (3) V. 1908, p. 218 - 220.

[23] Cauchy, Augustin de. „Rapport sur un mémoire de M. Lamé". C. R. 9. 1839, 1. p. 359—363 = Œuvres (1) 4. p. 499—504 = Journ. de Math. V. 1840, p. 211 —215.

[24] —— „Notes sur quelques propriétés des facteurs complexes". C. R. 24. 1847, 1. p. 347—349 = Œuvres (1) 10, p. 224—226.

[25] —— „Mémoires sur de nouvelles formules relatives à la théorie des polynomes radicaux et sur le dernier théorème de Fermat". C. R. 24. 1847, 1. p. 316, 469—481, 516—528, 578—584, 633—636, 661—666 = Œuvres (1) 10, p. 240 —285.

[26] —— „Mémoires sur diverses propositions relatives à la théorie des nombres". C. R. 25. 1847, 2. p. 132—136, 177—182, 242—243 = Œuvres (1) 10. p. 354 —368.

[27] Desboves, A. „Mémoires sur la résolution en nombres entiers de l'équation $aX^m + bY^m = cZ^n$". Nouv. Ann. Math. (2) 18. 1879, p. 265—279, 398—410, 433—444, 481—499.

[28] Dickson, L. E. (Berichtigung über L 178). L'Int. des Math. XV. 1908, p. 174.

[29] —— „On the last theorem of Fermat". Mess. of. Math. 38, 1908, p. 14—32.

[30] —— „On the last theorem of Fermat". Quart. Journ. 40. 1908, p. 27—45.

[31] —— „On the congruence $x^n + y^n + z^n \equiv 0$ (mod p)". Journ. für Math. 135, 1908, p. 134—141.

[32] —— „Lower limit for the number of sets of solutions of $x^e + y^e + z^e \equiv 0$ (mod p)". Journ. für Math. 135, 1909, p. 181—188.

[33] Dirichlet, P. G. Lejeune. „Mémoires lur l'impossibilité de quelques équations indéterminées du cinquième degré". Journ. für Math. 3. 1828, p. 354—375 = Werke I. p. 1—20, 21—46.

[34] —— „Démonstration du théorème de Fermat pour le cas des 14ièmes puissances". Journ. für Math. 9. 1832, p. 390—393 = Werke I. p. 189—194.

[35] —— „Bemerkungen zu Kummers Beweis für den Fermatschen Satz, die Unmöglichkeit von $x^\lambda - y^\lambda = z^\lambda$ für eine unendliche Anzahl Primzahlen betreffend". Mon.-Ber. Ak. Berlin 1847, p. 139—141 = Werke II. p. 254—255.

[36] Drach, S. M. „Proof of Fermat's undemonstrated theorem, that $x^n + y^n = z^n$ is only possible in whole numbers when $n = 1$ or 2". Phil. Mag. 27, 1845, p. 286—289.

[37] Dutordoir, H. „Sur une généralisation possible du dernier théorème de Fermat". Ann. Soc. Sci. Bruxelles 17. 1893, p. 81.

[38] Euler, Leonhard. „Theorematum quorundam arithmeticorum demonstrationes". Comm. Ac. Petrop. X. 1738. p. 125—146 = Comm. Arithm. I. p. 24—34.

[39] Euler, Leonhard. „Theoremata circa divisores numerorum". Novi Comm. Ac. Petrop. I p. 1747—48. p 20—48 = Comm. Arithm. I. p. 50—61.

[40] —— „Supplementum quorundam theorematum arithmeticorum quac in nonnullis demonstrationibus supponuntur". Novi Comm. Petr. VIII. 1760—61. p. 105—128 = Comm. Arithm. I. p. 287 - 296.

[41] —— Anleitung zur Algebra II. § 204, 234.

[42] —— „De divisoribus numerorum formae $a^n \pm b^n$". Tractatus de numerorum doctrina, cap. IX. Comm. Arithm. II. p. 533—535.

[43] Fermat, Pierre de. Diophanti Alexandri arithmethicorum libri sex, Tolosae 1670, Observatio Domini Petri de Fermat p. 61 = Œuvres I. p. 291, III. p. 241.

[44] Fleck, Albert (und Ph. Maennchen). „Vermeintliche Beweise des Fermatschen Satzes". Arch. Math. Phys. (3) 14. 1909. p. 284—286, 370—372.

[45] Gambioli, D. „Memoria bibliografia sull'ultimo teorema di Fermat". Per. di Math. 16 (2) III. 1901, p. 145—192.

[46] —— „Appendice alla mia memoria bibliografia . . . . .". Per. di Math. 17 (2) IV. 1902. p. 48—50.

[47] —— „Intorno all'ultimo teorema di Fermat". Il Pitagora 10, 1903—04, p. 11—13, 41—43.

[48] Gaudin. „Impossibilité de l'équation $(x+h)^n - x^n = z^n$". C. R. 59. 1864, 2. p. 1036—1038.

[49] Gauss, Karl Friedrich. „Zur Theorie der komplexen Zahlen" I. Werke II. p. 387—391. Handschriftlicher Nachlaß.

[50] Genocchi, Angelo. „Expressione generale de'numeri Bernoulli". Annali sci. mat. III. 1852, p. 395.

[51] —— „Intorno all'equazione $x^7 + y^7 + z^7 = 0$". Annali di Mat. VI. 1864, p. 287—288.

[52] —— „Généralisation du théorème de Lamé sur l'impossibilité de l'équation $x^7 + y^7 + z^7 = 0$". C. R 82, 1876, 1. p. 910—913.

[53] —— „Sur les nombres de Bernoulli". Journ. für Math. 99, 1886, p. 316—317.

[54] Germain, Sophie. Œuvres philosophiques. Paris 1879, p. 298—302.

[55] Gick, Christian. „Elementarer Beweis der Fermatschen Behauptung". Nürnberg 1908.

[56] Glaisher, John. W. L. „Note on Cauchy's theorem relating to the factors of $(x+y)^n - x^n - y^n$". Quart. Journ. XV. 1878, p. 365—366.

[57] —— „On Cauchy's theorem relating to the factors of $(x+y)^n - x^n - y^n$". Quart. Journ. XVI. 1879, p. 89—98.

[58] Gram, J. P. Förh. Skand. Naturf. 1898, p. 182.

[59] Grunert, Joh. Aug. „Wenn $n > 1$, so gibt es unter den ganzen Zahlen von 1 bis n nicht zwei Werte von x und y, für welche, wenn z einen ganzen Wert bezeichnet, $x^n + y^n = z^n$ ist". Arch. Math. Phys. 27, 1856, p. 119—120.

[60] Günther, S. „Über die unbestimmte Gleichung $x^3 + y^3 = a^3$". Sitz.-Ber. Böhm. Ges. Wiss. 1878, p. 112—120.

[61] Henry, C. „Recherches sur les manuscrits de Pierre de Fermat . . . . .". Bonc. Bull. XII. 1879, p. 477—568.

[62] Hess, Wilhelm. „Beweis des großen Fermatschen Satzes für ungrades $n > 1$". Dresden 1908 (A. Köhler).

[63] —— „Weiteres über den großen Fermatschen Satz". Dresden 1908 (A. Köhler).

[64] HILBERT, DAVID. „Die diophantische Gleichung $\alpha^m + \beta^m + \gamma^m = 0$". Die Theorie der algebraischen Zahlkörper. Kap. 36. Jahresber. D. Math.-Vergg. IV. 1894, p. 517—525.

[65] —— „Der FERMATsche Satz". Theorie des Kreiskörpers Nr. 14. Enz. math. Wiss. I, 2. p. 713—714.

[66] HOFFMANN, FRANZ. „Der Satz vom FERMAT. Sein seit dem Jahr 1658 gesuchter Beweis". (24 S.). Straßburg 1908 (J. SINGER).

[67] HÜBNER, A. „Über den FERMATschen Satz". (40 S.). Erlangen 1908 (F. JUNGE).

[68] JAQUEMET, CLAUDE. Bonc. Bull. XII. 1879, p. 565—568 (siehe L 61).

[69] JONQUIÈRES, ERNEST DE. „Sur le dernier théorème de FERMAT". Atti Acc. N. Lincei 37. 1884, p. 146—149.

[70] —— (Sur le dernier théorème de FERMAT) C. R. 98, 1884, 1. p. 863 864.

[71] —— „Sur une question d'algèbre qui a des lieus avec le dernier théorème de FERMAT". C. R. 120, 1895, 1, p. 1139—1143.

[72] JURISCH, KONR. W. „Beweis des FERMATschen Satzes". Berlin 1908 (C. HEYMANN) (Berichtigung s. L 44).

[73] KAUSLER, C. F. „Nova demonstratio theorematis nec summam, nec differentiam duorum biquadratorum biquadratum esse posse". Nova Acta Ac. Petrop. XIII. 1802, p. 237—244.

[74] —— „Nova ..... duorum cuborum cubum esse posse". N. Acta Ac. Petrop. XIII. 1802, p. 245—253.

[75] —— „Nova ..... duorum cubo-cuborum cubo-cubum esse posse". N. Acta Ac. Petrop. XV. 1806, p. 146—155.

[76] KLEIBER, JOH. „Das FERMATsche Problem". Aus Natur und Kultur. München 1908. V. p. 666—667.

[77] —— „Beitrag zum FERMATschen Satz". Zeitschr. math. nat. Unt. 40, 1909, p. 45—47.

[78] KOCH, J. „Beweis des großen FERMATschen Satzes". Borna-Leipzig 1908 (ROB. NOSKE).

[79] KORKINE, A. „Sur l'impossibilité de la relation algébrique $X^n + Y^n + Z^n = 0$". C. R. 90. 1880, 1. p. 303—404.

[80] —— (Über die Unmöglichkeit, der Gleichung $x^n + y^n + z^n = 0$ durch ganze Funktionen zu genügen) (Russisch) Nachr. Moskau X.

[81] KORNECK, G. „Beweis des FERMATschen Satzes von der Unmöglichkeit der Gleichung $x^n + y^n = z^n$ für rationale Zahlen und $n > 2$". Arch. Math. Phys. (2) 13. 1893, p. 1—9.

[82] —— „Nachtrag zum Beweis der FERMATschen Satzes". Arch. Math. Phys (2) 13, 1893, p. 263—267 (Berichtigung L 148 und Jahrb. Fortschr. Math. 1893, p. 134).

[83] KÜBLER, J. „Beweis des FERMATschen Satzes, daß die Gleichung $x^n + y^n = z^n$ für $n > 2$ in ganzen Zahlen niemals auflösbar ist". (18 S. mit 1 Tafel, 3 Fig.). Leipzig 1908. Esslingen 1908 (P. NEFF). (Berichtigung: L 44.)

[84] KUMMER, ERNST EDUARD. „De aequatione $x^{2\lambda} + y^{2\lambda} = z^{2\lambda}$ per numeros integros resolvenda". Journ. für Math. 17. 1837, p. 203—209.

[85] —— „Lettre à M. LIOUVILLE". Journ. de Math. 12. 1847, p. 136 = C. R. 24. 1847, 1, p. 899.

[86] —— „Allgemeiner Beweis des FERMATschen Satzes, daß die Gleichung $x^\lambda + y^\lambda = z^\lambda$ durch ganze Zahlen unlösbar ist, für alle diejenigen Potenzexponenten λ, welche

ungrade Primzahlen sind und in den Zählern der ersten $\frac{1}{2}(\lambda - 3)$ Bernoullischen Zahlen als Faktoren nicht vorkommen". Journ. für Math. 40. 1850, p. 130—138, siehe Mon.-Ber. Ak. Berlin 1847, p. 132.

[87] Kummer, Ernst Eduard. „Sur la théorie des nombres complexes composés de racines de l'unité et de nombres entiers". Journ. de Math. 16, 1851, p. 377—498.

[88] —— „Einige Sätze über die aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten komplexen Zahlen für den Fall, daß die Klassenzahl durch λ teilbar ist, nebst Anwendung derselben auf einen weiteren Beweis des letzten Fermatschen Satzes". Abh. Akad. Berlin 1857, p. 41—74. — Mon.-Ber. Ak. Berlin, p. 275—282.

[89] Lagrange, Joseph Louis. „Sur quelques problèmes de l'analyse de Diophante". Nouv. Mém. Berlin 1777 (1779), p. 140—154 = Œuvres IV. p. 377—398.

[90] Lamé, Gabriele. „Mémoire d'analyse indeterminée, démontrant que l'équation $x^7 + y^7 = z^7$ est impossible en nombres entiers". Journ. de Math. V. 1840, p. 195—211.

[91] —— „Mémoire sur le dernier théorème de Fermat". C. R. 9. 1839, 2. p. 45—46.

[92] —— „Mémoire sur la démonstration d'un nouveau cas du dernier théorème de Fermat". Mém. sav. étr. VIII. 1843, p. 421—437.

[93] —— „Mémoire sur la résolution en nombres complexes de l'équation $A^5 + B^5 + C^5 = 0$". Journ. de Math. 12. 1847, p. 137—171.

[94] —— „Mémoire sur la résolution en nombres complexes de l'équation $A^n + B^n + C^n = 0$". Journ. de Math. 12. 1847, p. 172—184.

[95] —— „Démonstration générale du théorème de Fermat sur l'impossibilité de l'équation $x^n + y^n = z^n$." C. R. 24. 1847, 1. p. 310—315, 352, 569—572, 588.

[96] —— „Études des binomes cubiques $(X^3 \mp Y^3)$." C. R. 61. 1865, 2. p. 921—924, 961—965.

[97] Landsberg, Otto. „Lettera al redattore" (Berichtigung von L 172). Giorn. di Mat. 28. 1890, p. 52.

[98] Lebesgue, Victor. „Note sur un théorème de Fermat." Journ. de Math. V. 1840, p. 184—185.

[99] —— „Démonstration de l'impossibilité de résoudre l'équation $x^7 + y^7 + z^7 = 0$ en nombres entiers." Journ. de Math. V. 1840, p. 276—279, 348—349.

[100] —— „Théorèmes nouveaux sur l'équation indéterminée $x^5 + y^5 = a z^5$." Journ. de Math. VIII. 1843, p. 49—70.

[101] —— „Résolutions des équations biquadratiques $z^2 = x^4 \pm 2^m y^4$; $z^2 = 2^m x^4 - y^4$; $2^m z^2 = x^4 \pm y^4$." Journ. de Math. 18, 1853, p. 73—86.

[102] Lefébure. „Sur la résolution de l'équation $x^n + y^n = z^n$ en nombres entiers." C. R. 90. 1880, 1. p. 1406—1407. (Berichtigung: L 142, Jahrb. Fortschr. Math. 1880.)

[103] Legendre, Adrien Marie. „Recherches sur quelques objets d'analyse indéterminée et particulièrement sur le théorème de Fermat." Mém. Ac. France 6. 1823, p. 1—60.

[104] —— Zahlentheorie II, (deutsch v. Maser, Leipzig 1893) Art 325—328, p. 4—8 ($n = 4$); Art. 331—333, p. 8—13 = L 103, p. 45—61 ($n = 3$); Art. 451, p. 118—120 (n allgemein); Art. 653, p. 348—352 = L 103, p. 41—45 ($n = 3$); Art. 654—663, p. 352—359 = L 103, p. 31—41 ($n = 5$).

[105] Libri, Guillaume. „Mémoire sur la théorie des nombres." Journ. für Math. 9. 1832, p. 54—80, 169—188, 261—276.

[106] Lindemann, Ferdinand. „Über den Fermatschen Satz betreffend die Unmöglichkeit der Gleichung $x^n = y^n + z^n$." Sitz.-Ber. Ak. München XXXI. 1901, p. 185—202. Berichtigung p. 495.

[107] —— „Über das sogenannte letzte Fermatsche Theorem." Sitz.-Ber. Ak. München. 37. 1907, p. 287—352.

[108] Liouville, Joseph. „Sur l'équation $Z^{2n} - Y^{2n} = 2X^n$." Journ. de Math. V. 1840, p. 360.

[109] —— „Observations sur le mémoire de M. Lamé." C. R. 24. 1847, 1, p. 315—316.

[110] Liouville, R. „Sur l'impossibilité de la relation algébrique $X^n + Y^n + Z^n = 0$." C. R. 89. 1879, 1. p. 1108—1110. (Berichtigung: Jahrb. Fortsch. Math. 11. 1879, p. 138 (Netto).)

[111] Lucas, Eduard. „Sur l'équation indéterminée $x^3 + y^3 = az^3$." Nouv. Ann. Math. (2) 17, 1878, p. 425—426.

[112] —— „Théorèmes généraux sur l'impossibilité des équations cubiques indéterminées." Bull. Soc. France. 8, 1880, p. 173—182.

[113] —— Théorie des nombres I. Paris 1891. Introduction p. XXIX.; p. 370—371, No. 206, Ex. VI; p. 267, No. 151, Ex. IV; p. 275, No. 157, Ex. II.

[114] Lucas, Felix. „Note relative à la théorie des nombres." Bull. Soc. Fr. 25, 1897, p. 33—35.

[115] Lukas, Franz. „Beweis, daß $x^n + y^n = z^n$ für $n > 2$ in ganzen Zahlen nicht auflösbar sei, nebst einer kurzen Auflösung für $n = 2$." Arch. Math. Phys. 58. 1876, p. 109—112. (Berichtigung: Jahrb. Fortschr. Math.)

[116] Mac Mahon, Percy Alexander. „Algebraic identities arising out of an extension of Waring's formula." Mess. of Math. 14. 1884. p. 8—11.

[117] Maillet, Edmond. „Le dernier théorème de Fermat." Assoc. franç. 26. 1897. p. 156—168.

[118] —— „Sur les équations indéterminées de la forme $x^\lambda + y^\lambda = cz^\lambda$." C. R. 129. 1899, 2. p. 198—199.

[119] —— „Sur les équations indéterminées de la forme $x^\lambda + y^\lambda = cz^\lambda$." Acta math. 24. 1901. p. 247—256.

[120] —— „Dernier théorème de Fermat $x^m + y^m \neq z^m$." Sur l'utilité de la publication de certains renseignements bibliographiques en mathématiques. C. R. du Congr. d. Math. Paris (1900). 1902. p. 425—427.

[121] —— „Sur les équations indéterminées $x^\lambda + y^\lambda = cz^\lambda$." Annali di Mat. (3) 12. 1905. p. 145—178.

[122] —— „Sur le dernier théorème de Fermat." Toulouse Mém. (10) V. 1905. p. 132—133.

[123] —— „Sur l'équation indéterminée $x^a + y^a = bz^a$." C. R. 140. 1905, 1. p. 1229—1230.

[124] Mansion, Paul. „Remarques sur les théorèmes arithmétiques de Fermat." Nouv. Corr. Math. V. 1879, p. 88—91, 122—125.

[125] —— (Bericht über den Wettbewerb) (s. L 18, 170) Bull. Ac. Belg. 52 (3) VI. 1883, p. 823—832.

[126] —— „Sur le dernier théorème de Fermat." Bull. Ac. Belg. (3) XIII. 1887, p. 16—17. Rectification p. 225.

[127] Martone, M. „Dimostrazione di un celebre teorema di Fermat." Catanzaro 1887. Neapel 1888

[128] —— „Nota a una dimostrazione di un ....." Neapel 1888.

[129] Mathews, G. B. „Note in connexion with Fermat's last theorem." Mess. of Math. XV. 1885, p. 68—74.

[130] —— „Note in connexion with Fermat's last theorem." Mess. of Math. (2) XXIV. 1894, p. 97—99.

[131] Metz, Jos. Edler von. „Beweis des Fermatschen Satzes." Göttingen 1908 (C. Spielmayers Nchf.).

[132] Mirimanoff, D. „Sur l'équation $x^{37} + y^{37} + z^{37} = 0$." Journ. für Math. 111. 1893, p. 26—30.

[133] —— „L'équation $x^l + y^l + z^l = 0$ et le critérium de Kummer." Journ. für Math. 128. 1905, p. 45—68.

[134] —— „Sur le dernier théorème de Fermat." L'Enseign. Math. XI. 1909, p. 49—51.

[135] Muir, Thomas. „On a expansion of $(x + y)^n + (- x)^n + (- y)^n$." Quart. Journ. XVI. 1879, p. 9—14.

[136] Neuberg, J. (Berichtigung von L 149 und L 168) Mathesis VIII. 1908, p. 243.

[137] Paulet, François. „Démonstration du théorème, dit de Fermat: Hors du second degré il n'existe aucune puissance qui puisse se partager dans la somme ou la différence de deux autres puissances du même degré." Quetelet, Corr. Math. XI. 1839, p. 307—313.

[138] —— „Démonstration du ..... degré." Cosmos 22, 1863, p. 385—389. (Berichtigung p. 407 v. R. Radau.)

[139] Penkmayer, Richard. „Beweis des Satzes von Fermat: die Gleichung $a^n + b^n = c^n$ ist in ganzen Zahlen unlösbar, wenn $n > 2$ ist." München 1908 (J. Lindauer). (Berichtigung: L. 44.)

[140] Pepin, Théophile. „Sur la décomposition d'un nombre entier en une somme de deux cubes rationels." Journ. de Math. (2) 15, 1870, p 217—236.

[141] —— „Impossibilité de l'équation $x^7 + y^7 + z^7 = 0$." C. R. 82, 1876, 1, p. 676—679, 743—747.

[142] —— „Sur divers tentatives de démonstration du théorème de Fermat." C. R. 91. 1880, 2, p. 366—368.

[143] —— „Mémoire sur l'équation indéterminée $x^3 + y^3 = Az^3$." Atti Acc. N. Lincei 34. 1881, p. 73—130.

[144] —— „Sur un théorème de Fermat." Atti Acc. N. Linc. 36. 1883, p. 23—33.

[145] —— „Étude sur l'équation indéterminée $ax^4 + by^4 = cz^2$." Atti Acc. N. Linc. 36. 1883, p. 34—70.

[146] Perrin, R. „Sur l'équation indéterminée $x^3 + y^3 = z^3$." Bull. Soc. Fr. 13 1884—85, p. 194—197.

[147] Pietzker, F. „Rationale Lösungen der Gleichung $x^n = y^n + z^n$." Unt.-Bl. Math. Nat. 14, 1908, p. 48—52. (Berichtigung L 44.)

[148] Poincaré, Jules Henry. „Rapport verbal ..... M. G. Korneck." (Berichtigung von L 81 und L 82) C. R. 118, 1894, 1, p. 841.

[149] Popoff, D. K. „Annexe à ma démonstration du théorème, dit „la Grande Proposition" de Fermat, à savoir que $a^n + b^n = c^n$ est impossible en nombres entiers." Sophia 1908. (Berichtigung: L 136 und L 44.)

[150] Réalis, S. „Sur quelques équations indéterminées du troisième degré." Nouv. Ann. Math. (2) 17, 1878, p. 454—457.

[151] Rieke, August. „Über die Gleichung $x^p + y^p = z^p$." Zeitschr. Math. Phys 34, 1889, p. 238—248.

[152] —— „Versuch über die Gleichung $x^p + y^p = z^p$." Zeitschr. Math. Phys. 36, 1891, p. 249—254. (Berichtigung von L 151 und 152: Zeitschr. Math. Phys. 37, 1892, p. 57, 64.)

[153] Rühl, Heinrich. „Elementarer Beweis des Fermatschen Satzes." (4 S.). Darmstadt 1908 (Müller & Rühle). (Berichtigung: L 44.)

[154] Sassé, E. „Fermats letzter Satz." Berlin 1908.

[155] Sauer, Richard. „Eine polynomische Verallgemeinerung des Fermatschen Satzes." Dissert. Giessen 1905.

[156] Schier, Otto. „Über die Auflösung der unbestimmten Gleichung $x^n + y^n = z^n$ in rationalen Zahlen." Sitz.-Ber. Wien. 1880, p. 392—398.

[157] Smith, Henry J. S. „Application to the Last Theorem of Fermat." Report on the Theory of Numbers. Part II, Art. 61 = Report of the British Association for 1860, p. 148—152 = Collected Math. Papers I. Oxford 1894, p. 131—137.

[158] Sommer, J. „Das letzte Theorem von Fermat." Vorlesungen über Zahlentheorie. Leipzig 1907, p. 176—193.

[159] Stäckel, Paul. „Beweis eines Satzes von Abel über die Gleichung $x^n + y^n + z^n = 0$." Acta math. 27, 1903, p. 125—128.

[160] Tafelmacher, W. L. Aug. „Sobre el teorema de Fermat de que la ecuacion $x^n + y = z^n$ no tiene solucion en numeros enteros x, y, z i siendo $n > 2$." Anales univ. Chile 82, 1892, p. 271—300, 415—437

[161] —— „Sobre la ecuacion $x^4 + y^4 = z^4$." Anales univ. Chile 84, 1893, p. 307 — 320.

[162] —— „La ecuacion $x^3 + y^3 = z^2$ i una demostracion del teorema de Fermat para el caso de las 6. potencias." Anales univ. Chile 97, 1897, p. 63—80.

[163] Tait, P. G. „On Fermat's theorem." Proc. Roy. Soc. Edinb. V, 1866, p. 181.

[164] —— „Mathematical Notes." Proc. Roy. Soc. Edinb. VII, 1872, p. 144.

[165] Talbot, William Henry Fox. „On Fermat's theorem." Trans. Soc. Edinb. 21, 1857, p. 403—406.

[166] —— „Remarks on Barlow's Theory of Numbers." On the Theory of Numbers, § 3. Trans. Soc. Edinb. 23, 1864, p. 51—52.

[167] Terquem, O. „Théorème de Fermat sur un trinôme." Nouv. Ann. Math. 6, 1847, p. 132—134.

[168] Théodoroff, P. „Démonstration de la grande proposition de Fermat, $x^n + y^n = z^n$ est impossible en nombres entiers, si $n > 2$." Sofia 1908 P. M. Basaitoff. (Berichtigung: L 44, 136.)

[169] Thue, Axel. „Et par bemerkninger vedrørende det Fermat'ske problem." Mindre middelsere. IV. p. 9—15, Arch. for Math. og Nat. 19, 1897, Nr. 4.

[170] Tilly, de. (Bericht über den Wettbewerb) (s. L 18, 125) Bull. Ac. Belg. 52 (3) VI. 1883, p. 820—823.

[171] Umfahrer, J. „Beweis der Richtigkeit des großen Fermatschen Satzes." München 1908 (O. Th. Scholl). (Berichtigung L 44.)

[172] Varisco, Dino. „Ricerche aritmetiche contenenti la dimostrazione generale del teorema di Fermat." Giorn. di Mat. 27, 1889, p. 371—380. (Berichtigung: L 96.)

[173] Vlachos, Chr. „Der Beweis des Fermatschen Satzes." Berlin 1908 (F. Gottheimer).

[174] Walsleben, A. „Der große Fermatsche Satz. Ein Versuch zur allgemeinen Lösung desselben." Osterode a Harz. (Selbstverlag.) (Berichtigung: L 44.)

[175] Weigelin, G. „Der große Fermatsche Satz und sein Beweis." 2 Teile (16 S. mit 1 Tafel) 1908, Stuttgart (H. Enderlin).

[176] Wendt, Ernst. „Arithmetische Studien über den „letzten" Fermatschen Satz, welcher aussagt, daß die Gleiehung $a^n = b^n + c^n$ für $n > 2$ in ganzen Zahlen nicht auflösbar ist." Journ. für Math. 113, 1894, p. 335—347.

[177] Werebrusow, A. („Über die Gleichung $x^5 + y^5 = Az^5$.") (Russisch) Mosk. Math. Samml. 25, 1905, p. 466—473.

[178] —— („Beweis") L'Interm. des Math. XV, 1908, p. 79—81. (Berichtigung p. 174—177, siehe L 28 und L 180.)

[179] Worms de Romilly, P. (Le dernier théorème de Fermat). L'Interm. des Math. II, 1895, p. 281 = XI, 1904, p. 185.

[180] —— (Berichtigung von L 178). L'Interm. XV, 1908, p. 176.

[181] N. N. „Versuch einer Lösung des großen Fermatschen Satzes. $a^n + b^n = c^n$." Halle und Leipzig 1908 (E. Karras).

[182] Nouv. Ann. Math. VIII, 1849, p. 362; IX, 1850, p. 386—392.

[183] Zeitschr. math. nat. Unt. 23, 1892, p. 417—418. „Die Gleichung $x^n + y^n = z^n$. Eine Anregung zur Auffindung eines Beweises."

4. Nachtrag.

(110)* Die Gleichung (1) ist in ganzen zu n primen Zahlen x, y, z unmöglich. Im Falle $n = 6m - 1$ muß eine dieser Zahlen durch $3n^2$ teilbar sein.

Herr WIEFERICH hat in seiner Arbeit „Zum letzten FERMATschen Theorem"[1]) gezeigt, daß die Annahme von ganzen nicht durch n teilbaren Zahlen x, y, z zu der Kongruenz $2^{n-1} \equiv 1 \pmod{n^2}$ führen muß.[2]) In der folgenden Untersuchung werde ich zeigen, daß die Unmöglichkeit von (1) in ganzen zu n primen Zahlen auf elementare Weise bewiesen werden kann.

Wegen (70), (75) und $(95,_{3,4})$ ist

$$(x + y)^n - x^n - y^n \equiv 0 \pmod{3^2}.$$

Ist keine der Zahlen x, y, z durch 3 teilbar, so kann man einen der beiden letzten Werte von (95) in diese Kongruenz einsetzen und man erhält für die dritte Gleichung von (95):

$$(3\alpha_1 + 3\beta_1 + 2)^n - (3\alpha_1 + 1)^n - (3\beta_1 + 1)^n \equiv 0 \pmod{3^2}$$

und nach der Potenzentwicklung:

$$(2^{n-1} - 1)[2 + 3\tbinom{n}{1}(\alpha_1 + \beta_1)] \equiv 0 \pmod{3^2}.$$

Da $2 + 3n(\alpha_1 + \beta_1)$ nicht durch 3 teilbar ist, so muß die Kongruenz

$$2^{n-1} \equiv 1 \pmod{3^2}$$

statthaben, was nur für $n = 6m + 1$ möglich ist.

Ist nun eine der drei Unbekannten, z. B. z, folglich auch c, durch 3, aber nicht durch n teilbar, so ergibt die Kongruenz (49):

$$nx^{n-1} \equiv \gamma^n \pmod{3^n}.$$

Nach (29) und (31) folgt dann

$$n \equiv 1 \pmod{3}.$$

Ist z aber auch durch n teilbar, so kann wegen (49a) diese Beschränkung nicht bestehen.

---

[1]) Journ. f. Math. 136, 1909, p. 293—302.

[2]) Ein Unmöglichkeitsbeweis dieser Kongruenz ist mir nicht bekannt.

Es kann demnach n bei ganzen zu n primen Zahlen x, y, z niemals von der Form $6m - 1$ sein. Im andern Falle kann n nur $= 6m - 1$ sein, wenn die durch n teilbare Zahl zugleich durch 3 teilbar ist. —

Bei nicht durch n teilbaren Zahlen führt (1) zu der Kongruenz (68):

$$(z + x_1)^n - z^n - x^n_1 \equiv 0 \pmod{n^2}.$$

Wenn aber ein Wert von x_1 gefunden ist, so läßt sich immer ein zweiter Wert x_2 ($\not\equiv x_1 \pmod{n}$) finden, der ebenfalls dieser Kongruenz genügt. Ich nehme jetzt an, daß alle Zahlen $< n$ sind, oder im andern Falle kongruent einer anderen Zahl modulo n gesetzt werden, die $< n$ ist. Die jetzt folgende Untersuchungsmethode zeige ich zuerst am Beispiel $n = 13$ und wähle die Kongruenz:

$$7^{13} - 2^{13} - 5^{13} \equiv 0 \pmod{13^2}.$$

Multipliziert man diese Kongruenz nacheinander mit allen Zahlen < 13, so erhält man 12 Lösungen < 13:

Multiplikant	z	x_1	$z + x_1$	Multiplikant	z	x_1	$z + x_1$
1*	2	5	7	7	1	9	10
2	4	10	1	8	3	1	4
3*	6	2	8	9	5	6	11
4	8	7	2	10	7	11	5
5	10	12	9	11	9	3	12
6	12	4	3	12	11	8	6

Da hierbei alle Zahlen < 13 vorkommen müssen, so erhält man für jede Zahl z, in diesem Falle für 2, noch eine zweite Kongruenz, bei der z (hier 2) an der Stelle von x_1 auftritt. Nun hat man zur Erlangung dieser Kongruenz die erste mit 3 multipliziert. Es ist dann

$$2 \cdot 2 \equiv 3 . 5 \times 2 \equiv 3 \cdot 2 \times 5 \equiv 6 \cdot 5 \pmod{13}.$$

Nimmt man statt 2 und 5 ein anderes der dargestellten Wertpaare von z und x_1, so erhält man durch Multiplikation wieder die genannten Lösungen, nur in anderer Reihenfolge. Da jede Zahl < 13 je einmal an der Stelle von z und x_1 vorkommt, so hat man für eine Zahl z immer zwei und nur zwei Zahlen x, die dieser Kongruenz genügen. Für den allgemeinen Fall von n ergibt sich dieselbe Konsequenz, da bei der Kongruenz

(111a) $$(z + x_1)^n - z^n - x^n_1 \equiv 0 \pmod{n^2}$$

noch eine zweite

(111b) $$(z + x_2)^n - z^n - x^n_2 \equiv 0 \pmod{n^2}$$

in ganzen Zahlen $< n$ existieren muß, und zwar findet man in der Tabelle mit Lösungen $< n$:

Multiplikant	z	x_1	$z + x_1$
1	z	x_1	$z + x_1$
. . . .	. . . .	. . . .	. . . .
r	$rz \equiv x_2$	$rx_1 \equiv z$	$r(x_1 + z) \equiv z + x_2$
. . . .	. . . .	. . . .	. . . .

Wie bei $n = 13$ hat man dann:

$$z^2 \equiv rx_1 \cdot z \equiv rz \cdot x_1 \equiv x_2 x_1 \pmod{n}.$$

Es besteht also für je zwei zusammengehörige Kongruenzen (111) die Kongruenz:

(112) $$z^2 \equiv x_1 x_2 \pmod{n}.$$

Bei der Existenz von (111) müssen aber auch die folgenden Kongruenzen bestehen:

$$[(n - x_1 - z) + z]^n - z^n - (n - x_1 - z)^n \equiv 0 \pmod{n^2}$$
$$[(n - x_2 - z) + z]^n - z^n - (n - x_2 - z)^n \equiv 0 \pmod{n^2}.$$

Es hat daher die (112) entsprechende Kongruenz statt:

$$z^2 \equiv (n - x_1 - z)(n - x_2 - z) \pmod{n}.$$

Die Kombination dieser Kongruenz mit (112) ergibt dann:

(113) $$z + x_1 + x_2 \equiv 0 \pmod{n},$$

und durch nochmalige Kombination erhält man:

(114) $$z^2 + zx_1 + x_1^2 \equiv 0 \pmod{n}.$$

Aus der Kongruenz

$$[(m_1 + m_2)n + z + x_1]^n - (m_1 n + z)^n - (m_2 n + x_1)^n \equiv 0 \pmod{n^2}$$

erhält man aber die Kongruenz (111a), also auch (114), und daher:

$$(m_1 n + z)^2 + (m_1 n + z)(m_2 n + x_1) + (m_2 n + x_1)^2 \equiv 0 \pmod{n}.$$

Für jede Kongruenz (111a) in ganzen nicht durch n teilbaren Zahlen $\gtrless n$ besteht demnach immer (114). —

Nun geht aus (1) wie bei (68) die Kongruenz hervor:

$$(z - x)^n - z^n - (-x)^n \equiv 0 \pmod{n^2}.$$ [1]

Man hat deshalb

$$z^2 - zx + x^2 \equiv 0 \pmod{n}$$

oder wegen (8)

$$x^2 + xy + y^2 \equiv 0 \pmod{n}.$$

---

[1]) Da

$$(z - y)^n - z^n - (-y)^n \equiv 0 \pmod{n^2},$$

und y nicht gleich x, so ist $y \equiv x_2$, wonach (113) durch $z - y - x \equiv 0 \pmod{n^2}$ bestätigt wird.

Nach (19) ist

$$x \equiv a, \quad y \equiv b \pmod{n^{\lambda - 1}},$$

wobei zunächst $\lambda - 1 = 1$ sei. Dann hat man:

$$a^2 + ab + b^2 = a^2 + b(a + b) \equiv 0 \pmod{n^{\lambda - 1}}$$

und durch Potenzierung:

$$(a^2)^n + b^n (a + b)^n \equiv 0 \pmod{n^\lambda}.$$

Nun ist nach (8) und (20):

$$c \equiv a + b \pmod{n^{\lambda - 1}}$$

oder

$$c^n \equiv (a + b)^n \pmod{n^\lambda}.$$

Wegen (8) ist aber:

$$c^n \equiv a^n + b^n \pmod{n^\lambda},$$

folglich

$$(a + b)^n \equiv a^n + b^n \pmod{n^\lambda}$$

und

$$a^{2n} + b^n (a^n + b^n) = a^{2n} + a^n b^n + b^{2n} \equiv 0 \pmod{n^\lambda}.$$

Die Kongruenzen (11)

$$x \equiv a^n, \quad y \equiv b^n \pmod{n^\lambda}$$

ergeben dann:

$$x^2 + xy + y^2 \equiv 0 \pmod{n^\lambda}.$$

Nun habe ich im vorangegangenen gezeigt, daß n nicht $= 6m - 1$ sein kann. Sei daher n von der Form $6m + 1$, so wird wegen (70):

$$(x + y)^n - x^n - y^n \equiv 0 \pmod{n (x^2 + xy + y^2)^2}$$

$$\equiv 0 \pmod{n^{2\lambda + 1}}$$

oder

$$(x + y)^n - z^n \equiv 0 \pmod{n^{2\lambda + 1}}.$$

Nach Satz (2) ergibt sich dann:

$$x + y - z \text{ oder } c^n - b^n - a^n \equiv 0 \pmod{n^{2\lambda}}.$$

In den Gleichungen von (3) bis (20) ist also λ zu 2λ geworden. Es folgt demnach wiederum aus (8) und (20):

$$c \equiv a + b \pmod{n^{2\lambda - 1}}.$$

Da

$$x^2 + xy + y^2 \equiv 0 \pmod{n^\lambda}$$

und jetzt

$$x \equiv a, \quad y \equiv b \pmod{n^\lambda}$$

ist, so erhält man wie oben nacheinander:

$$a^2 + ab + b^2 \equiv 0 \pmod{n^\lambda}$$

$$a^{2n} + b^n (a + b)^n \equiv 0 \pmod{n^{\lambda + 1}}$$

$$a^{2n} + a^n b^n + b^{2n} \equiv 0 \pmod{n^{\lambda+1}}$$
$$x^2 + xy + y^2 \equiv 0 \qquad ,,$$
$$(x+y)^n - z^n \equiv 0 \pmod{n^{2\lambda+3}}$$
$$c^n - b^n - a^n \equiv 0 \pmod{n^{2\lambda+2}}$$
$$c \equiv a + b \pmod{n^{2\lambda+1}},$$
$$a^2 + ab + b^2 \equiv 0 \pmod{n^{\lambda+1}}$$
$$x^2 + xy + y^2 \equiv 0 \pmod{n^{\lambda+2}}$$

. . . .

usw. bis zu

$$x + y - z \equiv 0 \pmod{n^\infty},$$

was nur möglich wäre, wenn

$$x + y - z = 0,$$

dies wegen (1) aber ausgeschlossen ist. —

Die Unmöglichkeit von (1) in ganzen zu n primen Zahlen kann für $n = 6m - 1$ auch auf folgende Weise bewiesen werden.

Für $x_1 = -x$ erhält man aus (114):

$$(z+x)(z^2 - zx + x^2) = z^3 + x^3 \equiv 0 \pmod{n}.$$

Da $z^3 + x^3$ in $z^{3(2m-1)} + x^{3(2m-1)}$ enthalten ist, so hat man auch:

$$z^{6m-3} + x^{6m-3} \equiv 0 \pmod{n},$$

und nach Multiplikation mit zx:

$$xz^{6m-2} + zx^{6m-2} \equiv 0 \pmod{n}.$$

Es ist aber

$$x^{n-1} = x^{6m-2} \equiv z^{6m-2} \equiv 1 \pmod{n};$$

folglich ergibt die vorhergehende Kongruenz:

$$x + z \equiv 0 \pmod{n}.$$

Ebenso erhält man:

$$z + y \equiv 0 \pmod{n}.$$

Durch Addition dieser beiden Kongruenzen wird dann:

$$2z + x + y \equiv 0 \pmod{n},$$

und man hätte wegen (4) die Kongruenz:

$$3z \equiv 0 \pmod{n},$$

die aber der Voraussetzung widerspricht.

686





